H3C MSR 系列路由器 NAM 网络分析模块

用户手册

杭州华三通信技术有限公司

http://www.h3c.com.cn

资料版本：20070425-C-1.00

产品版本：NAM VER 1.00

声明

H3C、H3C、Aolynk、Aolynk、H^{3}Care、H3Care、TOP G、TOPG、IRF、NetPilot、Neocean、NeoVTL、SecPro、SecPoint、SecEngine、SecPath、Comware、Secware、Storware、NQA、VVG、V^{2}G、V^{n}G、PSPT、XGbus、N-Bus、TiGem、InnoVision、HUASAN、华三均为杭州华三通信技术有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。如需要获取最新手册，请登录 http://www.h3c.com.cn。

技术支持

用户支持邮箱：customer_service@h3c.com

技术支持热线电话：800-810-0504（固话拨打）

400-810-0504（手机、固话均可拨打）

网址：http://www.h3c.com.cn

前 言

相关手册

手册名称	用途
《H3C MSR 系列路由器 OAP 单板手册》	对用户安装和配置 MSR 系列路由器 OAP 单板进行指导。
《H3C MSR 系列路由器 NAM 网络分析模块软件 安装手册》	介绍 NAM 网络分析软件的安装操作指导。

本书简介

本手册各章节内容如下：

- **第 1 章 产品概述**。介绍 NAM 产品的软硬件基本情况以及 NAM 产品的功能特点。
- **第 2 章 安装指导**。介绍使用 NAM 产品所必需的硬件连接、软件配置。
- **第 3 章 配置指南**。介绍 NAM 产品的界面概况，以及在实际环境中的典型应用。
- **第 4 章 常见问题解答**。介绍在使用 NAM 产品过程中可能会遇到的特殊情况，以及对应的解决办法。
- **附录 A NAM 软件功能详解**。介绍 NAM 产品每一个菜单的功能概况和功能细节，便于用户查询。

本书约定

1. 命令行格式约定

格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。

格　式	意　义
{ x | y | ... } *	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...] *	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入 1～n 次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

小心、注意：提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。

警告：该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。

说明、提示、窍门、思考：对操作内容的描述进行必要的补充和说明。

环境保护

本产品符合关于环境保护方面的设计要求，产品的存放、使用和弃置应遵照相关国家法律、法规要求进行。

目 录

第1章 产品概述

1.1 NAM 介绍

NAM（Network Analysis Module）是网络分析模块的简称，是 H3C 公司在 MSR 系列路由器设备上开发的流量监控软硬件平台。使用 NAM 单板，用户可以把流经路由器的所有流量进行统计和分析，为网络管理员提供网络安全服务。

NAM 单板有 MIM-NAM 和 FIC-NAM 两种类型，MIM-NAM 在 MSR 30 系列路由器上使用，FIC-NAM 在 MSR 50 系列路由器上使用。

NAM 单板对外提供 1 个管理用的 GE 电口、2 个 USB 接口；同时提供 80G 硬盘存储空间。

MIM-NAM 的面板如下图所示：

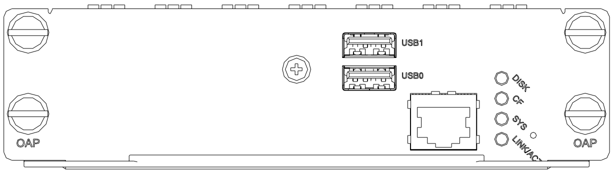


图1-1 MIM-NAM 面板

FIC-NAM 的面板如下图所示：

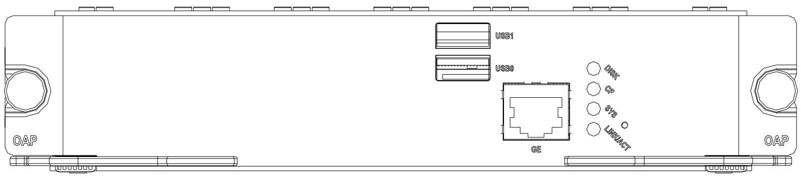


图1-2 FIC-NAM 面板

NAM 用于监控路由器的流量，由于路由器在网络中得天独厚的位置，使任何内 Internet 通讯的流量都会经过路由器设备，也就是使 NAM 能够获取最为全面的流量数据，提供出更加准确和详细的网络流量分析结果。

NAM 产品提供了如下主要功能：

- 支持对路由器所有出入三层端口网络流量的分析，并且支持定制分析端口。
- 支持在线流量的网络流量分析。
- 支持对网络流量采样记录和对历史流量进行网络流量分析。
- 支队对多种网络协议分析，包括 IP/none-IP 的、2 至 7 层的协议，多达百余种。

- 支持对网络协议的过滤分析。
- 方便友好的用户配置，支持图形化的分析结果查询。

同时，NAM 采用基本功能＋插件的方式，为功能的可扩展提供了有力的保障，也为进一步满足用户需求做好了准备。

1.2 NAM 应用介绍

NAM 通过对网络流量的分析和统计，真实的反映了网络的具体情况，有助于网络管理员及时了解和定位各种网络异常。网络管理员可以使用 NAM 的以下四种应用来提高网络的安全性和健壮性：

- 路由器流量镜像－－获取路由器的网络流量信息
- 网络流量统计——分析各种网络事件
- 网络流量监控——及时发现网络事件
- 网络安全漏洞检测——消除隐患的有力武器
- 网络的优化与规划——带来一个更合理、更健壮、更安全的网络

1.2.1 路由器流量镜像

路由器物理接口类型丰富，链路层帧格式各不相同，只能通过软件将 IP 报文进行镜像才能获得流量信息。NAM 软件可以配置路由器，将路由器接口上的进出流量镜像到 NAM 单板，为进行路由器的网络流量分析提供数据源。

1.2.2 网络流量统计

NAM 支持对网络中的主机进行流量统计。只要能获取主机的名称、MAC 地址或 IP 地址，NAM 就能对该主机发送和接收的流量进行统计。

NAM 可以统计的网络流量包括：网络总流量、IP 组播流量、TCP/UDP 流量。统计的同时，NAM 实时对流量进行处理和分析，形成其他附加信息，包括：TCP/UDP 服务、主机操作系统信息、带宽使用情况和流量分布情况。

1. 对总流量的统计

基于各种协议发送和接收的数据的总流量，协议包括各层协议，如网络层协议 IP、IPX、应用层协议 FTP、HTTP 等。

2. 对 IP 组播流量的统计

发送和接收的 IP 组播数据的总流量。

3. 对 TCP 会话及其流量、UDP 流量的统计

(1) 当前处于活跃状态 TCP 会话，以及与每个会话对应的流量。

(2) 通过端口号识别各种 UDP 流量。

4. 对 TCP/UDP 服务的识别

通过主机正在监听或使用的端口号，识别主机使能的 TCP/UDP 服务。

5. 对操作系统信息的识别

识别主机的操作系统，包括 Microsoft Windows、Unix/Linux 等常用操作系统。

6. 对带宽使用情况的统计

主机的即时流量、流量平均值和峰值。

7. 对流量分布情况的统计

本地流量（主机与同一个子网内的其他主机的流量）和本地－远程流量（主机与其他子网主机的流量）的流量分布。

8. 对 IP 流量分布情况的统计

TCP 和 UDP 的流量分布。

1.2.3 网络流量监控

网络流量数据包含了网络运行状况的信息，优秀的网络管理员通过这些数据，可以了解网络的使用情况，找出不符合当前网络配置的主机或其他故障点。在 NAM 网络流量统计功能的基础上，主要可以发现以下几类网络配置问题：

1. 主机掩码配置错误

NAM 可以监控网络中所有的子网信息，从而发现配置错误掩码的主机。

2. 服务的错误配置和使用

通过监控网络中各种服务的报文收发情况，特别是请求报文的频繁发送，可以分析网络中的主机使用这些服务时配置是否正确。

3. 无效协议

通过查看报表中的协议，可以发现不能在网络中正常使用的协议，如网络中正在使用 TCP/IP 协议，而某些主机安装了 IPX、AppleTalk 等协议，这些协议不但不能正常使用，还会产生一些无效流量，浪费网络资源。

4. 网络资源的不合理分配

通过监控网络带宽使用情况，可以分析网络中占用大量带宽、消耗大量网络资源的主机及其使用的服务。

1.2.4 网络安全漏洞检测

网络安全已经成为网络管理员最关注的问题之一。通常情况下，网络的安全隐患源于网络中存在的漏洞。而漏洞分为两个方面：第一，主机自我保护存在缺陷，容易被攻击；第二，网络中有人利用便利的网络资源，对网络中的其他主机实施攻击。

NAM 通过对网络安全漏洞的检测，可以发现缺乏自我保护能力的主机和对外实施攻击的主机，为网络管理员采取针对性措施提供依据。

NAM 能检测的安全漏洞包括：

- 端口扫描（Portscan）检测
- 欺骗攻击（Spoofing）检测
- 木马（Trojan horse）检测
- 拒绝服务（DoS）攻击检测

1.2.5 网络的优化与规划

网络的性能也是网络管理员关注的焦点。通常情况下，不是硬件导致网络性能不良，而是对网络不合理的配置与使用导致了带宽浪费。NAM 通过对网络流量的分析，可以协助管理员优化网络，或者在局部重新规划网络，从而使网络性能上一个台阶。

NAM 能探知的网络不合理使用包括：

(1) 识别无效的网络协议，减少网络流量

前面已经提到，通过查看报表，可以发现主机安装的无效网络层通信协议，如 IPX 等。

另外，OSPF、IGMP 等协议需要在一定范围内使用才能发挥作用。NAM 收集协议的流量，并以此分析这些协议是否只是在网络中零星、孤立的主机上使用。网络管理员根据分析的结果采取相应的措施（如关闭特定的协议）来减少网络中的无效流量。

(2) 识别冗余的网络协议，减少网络流量

在网络中，为了实现同一种功能，有时会使用多种协议，浪费了网络带宽资源，如全部服务器都使用 DNS 服务，而又有少量服务器同时使用 WINS 服务。NAM 可以提供协议报表，为网络管理员去除冗余协议提供依据。

(3) 识别多余连接，节省网络资源

在网络中，适当的设置代理能减少主机之间的连接数，减少多余连接，节省网络资源。NAM 可以提供网络连接的报表，为网络管理员合理设置代理提供参考。

(4) 优化路由

NAM 可以获取 ICMP 重定向消息来发现网络中的次优路由。网络管理员可以根据这一信息来优化网络中的路由。

(5) 优化网络结构

NAM 可以收集流量并把流量与协议、流向相关联。网络管理员根据这些数据可以分析网络中的服务器（DNS、DHCP）位置是否合理，并作出适当调整。

第2章 安装指导

2.1 安装准备

请参考表 2-1中所示的各个检测项目，确保安装NAM软件的条件均已具备。

表2-1 安装环境确认

检测项	检测标准
路由器	检查路由器是否提供 NAM 单板插槽。 若已提供，本安装条件已经具备。
NAM 单板	检查 NAM 单板是否符合合同的规定（包括 NAM 单板型号及版本、NAM 主机软件版本、NAM 软件版本）。 符合合同的规定表示检查合格，本安装条件已经具备。
PC	PC 是否安装了网卡并根据实际组网配置 IP 地址；PC 是否安装了网页浏览器应用程序，如 IE 6.0。 若已安装，本安装条件已经具备。

只有上述三个检测项都通过，安装 NAM 软件的条件才具备。

📖 说明：

NAM 软件的使用依赖于路由器的基本功能。在使用 NAM 软件时，请确保路由器在网络中处于正常运行状态。

2.2 硬件的安装和连接

📖 说明：

在安装 MIM-NAM 单板之前，请先切断路由器的电源。

2.2.1 安装 NAM 单板

将 NAM 单板完全插入路由器的 NAM 单板插槽，并固定。

2.2.2 连接 NAM 单板和 PC

NAM 单板和 PC 可以通过交叉网线直连，也可以通过网络连接。为 NAM 单板的以太网口和 PC 配置 IP 地址后，只要 PC 和 NAM 单板路由可达，即可在 PC 上通过 IE 访问 NAM 软件。

2.3 NAM 的简单配置

按照上述步骤进行操作之后，要使 NAM 软件能够正确实现其监控功能，仍需要对设备和 NAM 软件进行一些设置。

2.3.1 登录 NAM 管理页面

确认PC自动获取了IP地址之后，使用PC上的IE浏览器访问http://192.168.0.1。IE浏览器弹出NAM登录窗口，如图 2-1所示。

说明：

NAM单板网络管理接口的IP地址出厂设置为 192.168.0.1，掩码为 255.255.255.0。此IP地址可通过NAM管理页面进行设置，请参见2.3.2 配置NAM的内部接口和管理接口IP地址。



图2-1 NAM 登录窗口

输入缺省的用户名 admin 和密码 admin，进入 NAM 管理页面，如图 2-2 所示。

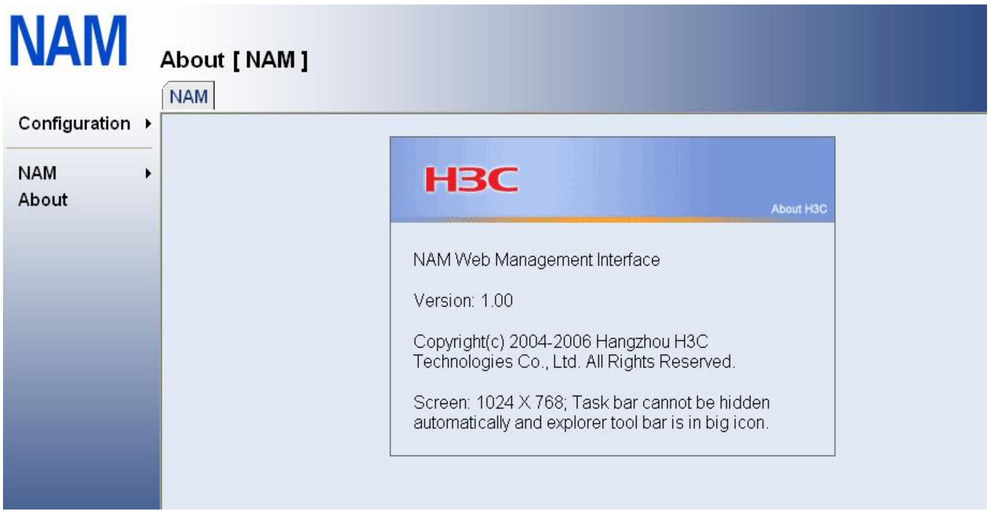


图2-2 NAM 配置页面

2.3.2 配置 NAM 的内部接口和管理接口 IP 地址

NAM 前面板的接口是管理接口。用来与网络设备进行数据交互的接口为内部接口。

说明：

- 此步骤可省略。如果没有修改 NAM 内部口 IP 地址，则 IP 地址默认为 192.167.0.11；如果没有修改 NAM 的管理口 IP 地址，则此 IP 地址默认为 192.168.0.1
- NAM 上与路由器进行数据交互的接口的地址称为本地 IP 地址。路由器上与 NAM 进行数据交互的接口的 IP 地址称为关联 IP 地址。因此，我们需要事先在路由器上配置好与 NAM 相连的接口的地址，再把这个地址填入到关联 IP 地址栏中。本地 IP 地址必须与关联 IP 地址处于同一网段，而且它们两个不能和管理 IP 地址处于同一网段。

单击导航树中的[Comfiguration/NICs IP Address]菜单项，即可进入配置NAM内部口和管理口IP地址页面，如图 2-3所示。

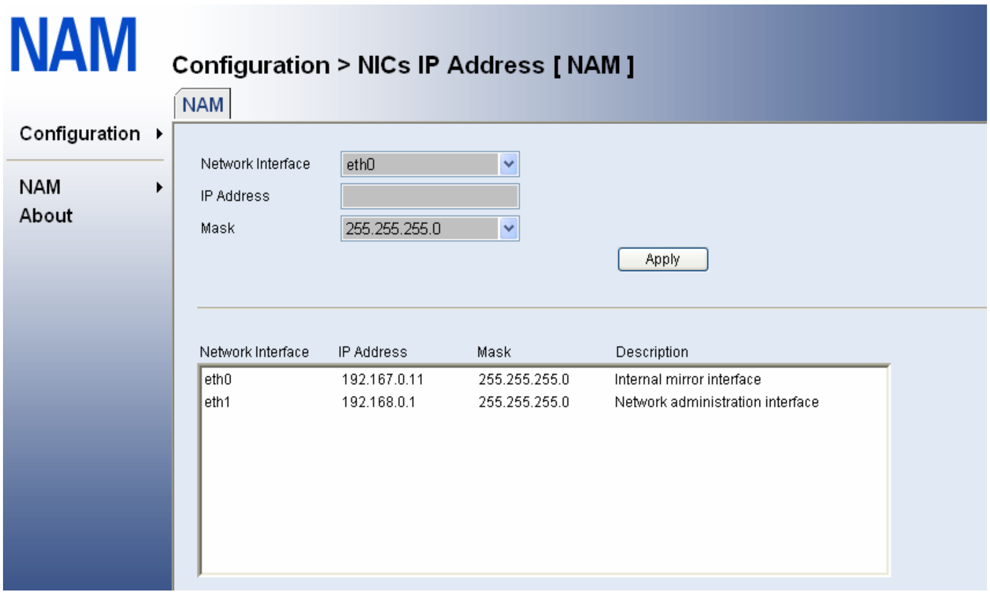


图2-3 NAM 管理 IP 地址配置页面

在页面上方可以配置 NAM 的内部口和管理口 IP，配置的结果将在页面下方的提示信息框中显示。

输入适当的 IP 地址，选择正确的掩码，单击<Apply>按钮即可完成配置。

说明：

修改 NAM 的管理口 IP 后，必须使用 IE 浏览器访问新配置的 IP 地址才能再次登录 NAM。

2.3.3 设置登录密码

说明：

缺省的用户名和密码均为 admin。建议首次登录后，立即更改登录密码。

单击导航树中的[Comfiguration/Web Admin Password]菜单项，即可进入登录密码设置页面，如图 2-4所示。

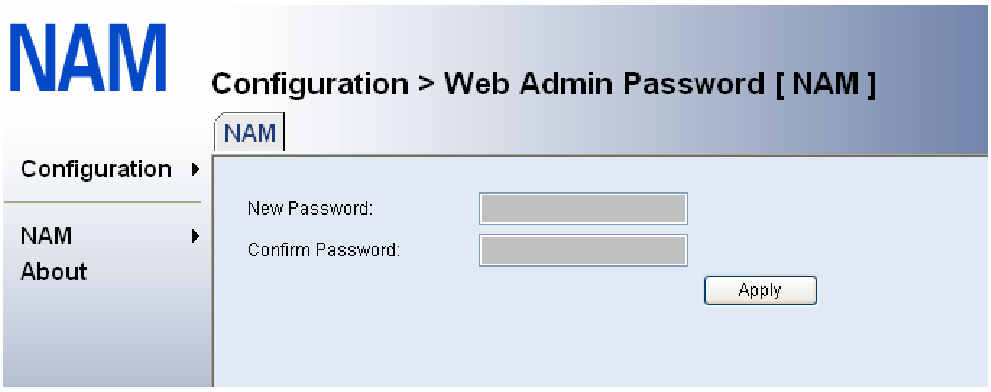


图2-4 设置登录密码页面

输入两遍新的密码后，单击<Apply>按钮即可完成操作。

说明：

设置新的登录密码后，再次进入其他管理页面时，会弹出登录窗口。只有输入新设置的密码才能正常进入下一步。

2.3.4 SNMP 参数配置

NAM 软件需要通过 SNMP 协议来配置路由器接口的流量镜像，SNMP 相关参数必须配置正确，才能配置路由器接口的流量镜像。

单击导航树中的[Configuration/Traffic Mirror/SNMP Preferences]菜单项，即可进入 NAM 软件 SNMP 参数配置页面，如下图所示。

“SNMP Protocol Version”为 SNMP 协议的版本号，目前只支持 v2c；“Remote SNMP Agent”为 NAM 单板路由器侧 GE 口的 IP 地址；“Read Community”和“Write Community”分别为路由器配置的 SNMP 读和写团体字。

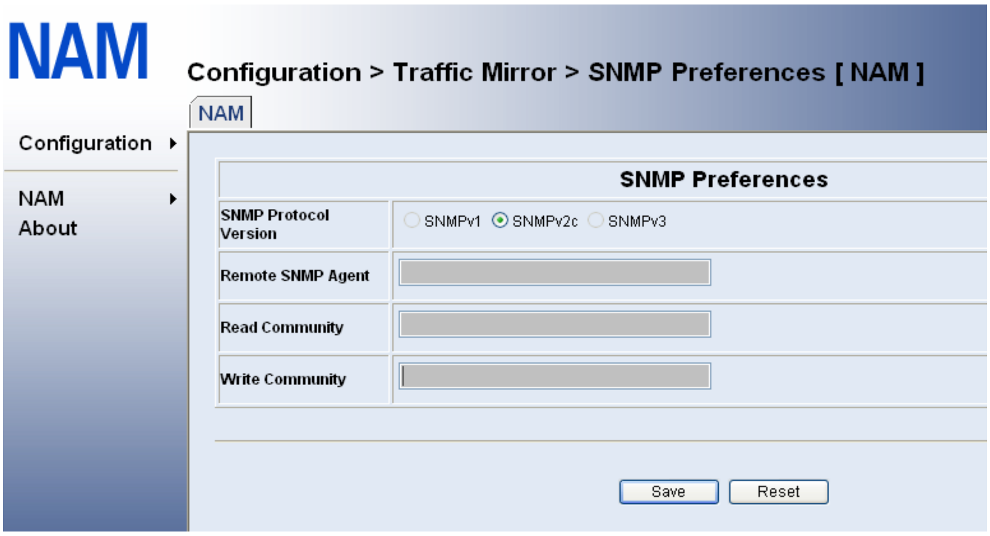


图2-5 SNMP 参数配置页面

2.3.5 路由器接口流量镜像配置

路由器接口的流量默认不进行镜像，NAM 软件通过 SNMP 协议配置路由器将接口流量镜像到 NAM 软件，才能对路由器接口的流量进行分析。

单击导航树中的[Configuration/Traffic Mirror/Mirror Interface]菜单项，即可进入 NAM 软件路由器接口流量配置页面，如下图所示。

“Traffic Mirror”中的“Enable”和“Disable”分别表示使能或禁止流量镜像。当选择使能流量镜像时，NAM 软件根据用户选择的流量镜像的源接口和 NAM 单板所在的槽位号来配置路由器；当选择禁止流量镜像时，NAM 软件配置路由器，删除所有已配置流量镜像的源接口，不再对路由器的接口流量进行镜像。

“Mirror Source Interface”左边显示路由器所有可以进行流量镜像的接口；右边显示已配置流量镜像的接口。用户可以根据需要将左边列表中的接口添加到右边；也可以将右边列表中的接口添加到左边。

“Mirror Destination Subslot”为 NAM 单板所在的槽位号，只有正确的配置该槽位号，NAM 软件才能正确的配置路由器接口流量。

上述信息配置正确后，点击“Apply”按钮，对路由器接口流量镜像的配置就可以生效了。

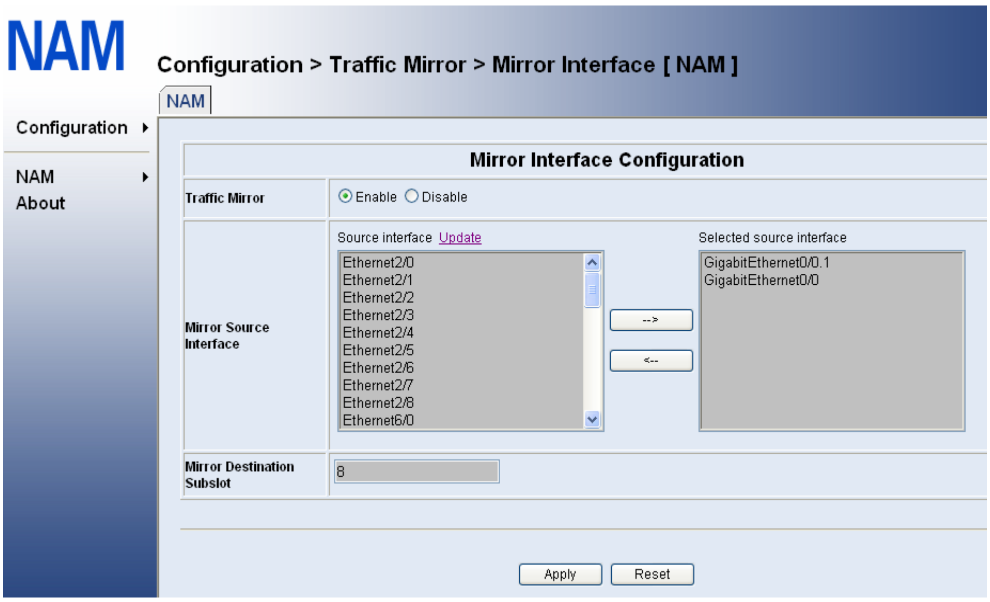


图2-6 启动和关闭 NAM 软件页面

2.3.6 启动和关闭 NAM 软件

单击导航树中的[NAM/Administration]菜单项，即可进入NAM软件的启动和关闭界面，如图 2-7所示。

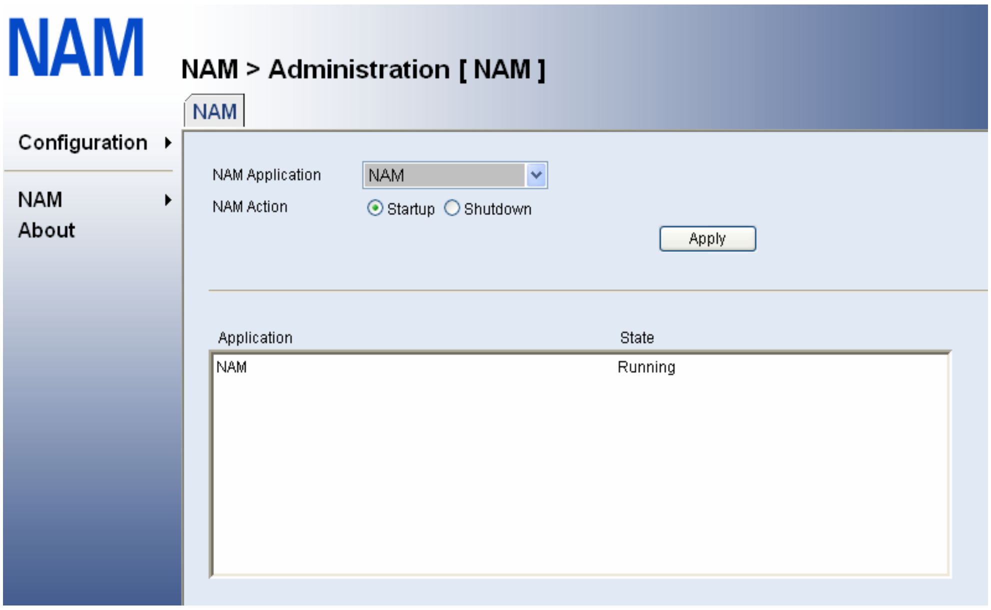


图2-7 启动和关闭 NAM 软件页面

对 NAM 软件的操作有两种：Startup 和 Shutdown。执行这两种操作后，对应的 NAM 软件的运行状态分别为 Running 和 Stop。NAM 软件当前的运行状态将在下方实时显示。

2.3.7 打开 NAM 监控页面

目前提供 HTTP 和 HTTPS 两种方式来访问 NAM 监控页面。

单击导航树中的[NAM/Monitor(HTTP)]或[NAM/Monitor(HTTPS)]菜单项，即可进入NAM监控页面，如图 2-8所示。

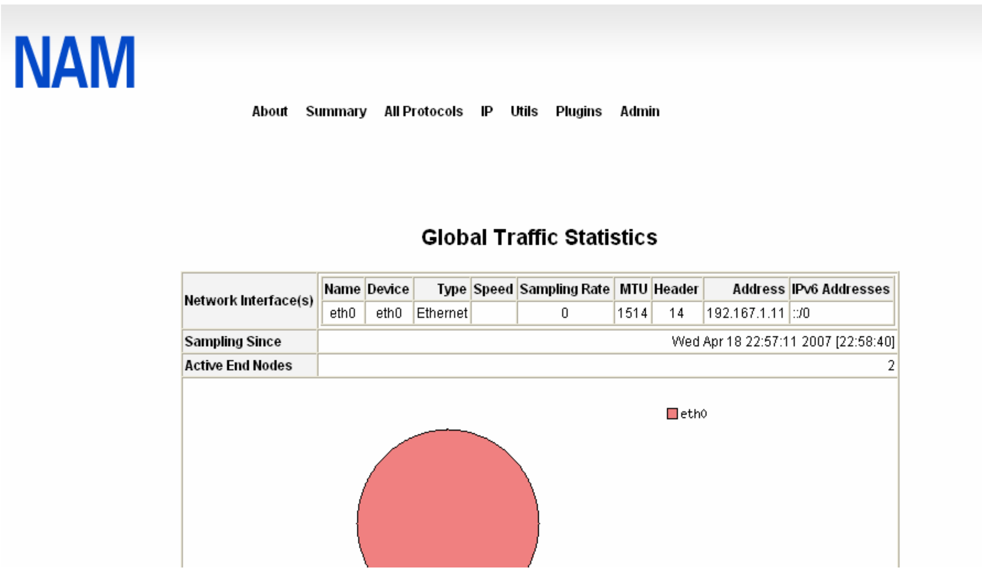


图2-8 NAM 软件监控页面

NAM 监控页面中提供了丰富的菜单项，方便网络管理员进行各种网络流量和网络信息的查看，帮助网络管理员实现网络流量统计、网络安全漏洞检测、网络优化和规划等强大功能。NAM 监控页面的具体使用请参见本文第三章的相关内容。

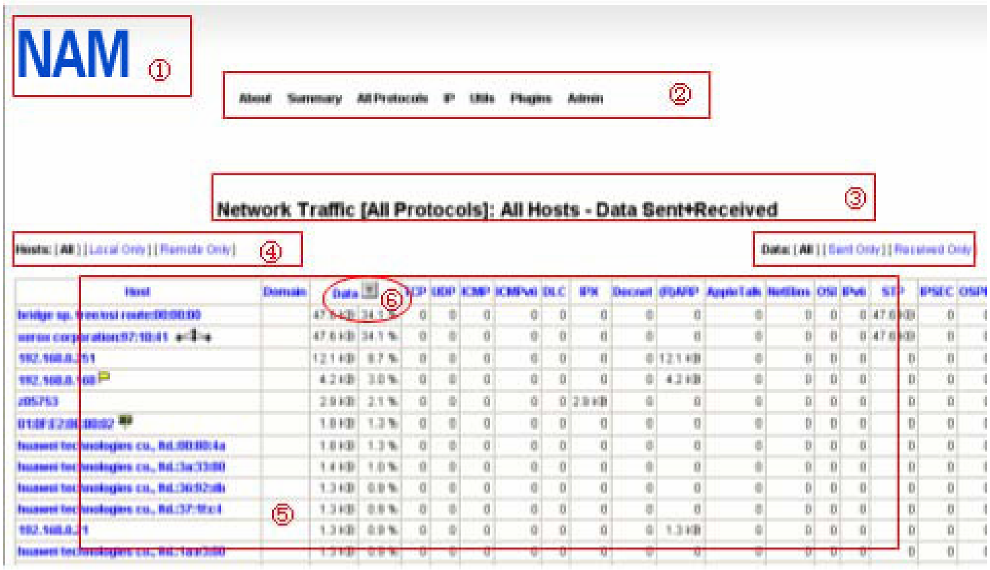
第3章 配置指南

3.1 NAM 主要界面简介

在使用 NAM 的过程中，网络管理员可以查看各种数据统计界面来对流量进行分析。下文将介绍 NAM 系统中常用的数据统计界面。

3.1.1 界面概述

NAM界面的布局都采用统一的风格，类似于图 3-1。



①：产品 Logo。
②：功能菜单：用于进入不同的NAM报表界面和NAM配置界面。详细说明请参见表 3-1
③：当前界面的标题。
④：功能链接：用于切换当前界面显示的内容。
⑤：显示界面：NAM 窗口的主体，用于显示 NAM 报表或 NAM 配置项。
⑥：排序功能：点击表单中的表头，表单将按照该表头的顺序或逆序进行排序。

图3-1 界面布局示例

表3-1 功能菜单说明

功能菜单项	子项	相关说明
About	What is NAM	介绍 NAM 的基本功能
	Show Configuration	显示 NAM 当前配置以及进程相关信息
	Risk Flags	说明风险标识的含义
	About NAM	NAM 版权说明

功能菜单项	子项	相关说明
Summary	Traffic	此界面显示了网卡探测到的所有流量的信息
	Hosts	此界面显示了主机信息，分别以字节、报文为单位显示，同时又可以基于 VLAN 来查看不同的主机信息。更强大的功能是，它每一列都支持排序，方便用户很快的查询到所需要的信息
	Network Load	本页面主要是显示的被监控接口的网络负载情况
	VLAN Info	此界面主要是基于 VLAN 统计了流量的大小
	Network Flows	此界面主要显示了 Host Last Seen 插件和用户自定义的流规则的流量情况
All Protocols	Traffic	此界面包含了所有协议的网络流量情况，包括所有主机的发送和接收报文情况
	Throughput	此界面下面包含了所有协议的网络负载情况，包括所有主机的发送和接收报文情况
	Activity	此界面下面包含了所有协议的网络活动情况
IP	Summary	主要统计各种应用层协议信息
	Traffic Directions	记录内网和外网各个流向的流量统计
	Local	记录本地的端口号，TCP 连接以及主机操作系统信息
Utils	Data Dump	导出数据和日志
	View Log	查看日志
Plugins	Host Last Seen	记录 NAM 最后一次捕获到本地主机报文的时间
	ICMP Watch	统计 ICMP 报文信息
	NetFlow	收集和分析 NetFlow 报文
	PDA	网络的简单统计信息
	Round-Robin Databases	保存和查看历史流量信息
	sFlow	收集和分析 NetFlow 报文
	All	集中显示各个插件的状态

功能菜单项	子项	相关说明
Admin	Switch NIC	切换网络接口
	Configure	更改 NAM 系统级配置，包括下次启动的配置参数，当前的配置参数，以及安全策略
	Shutdown	关闭 NAM

后续进行界面介绍时，以上提到的部分不再赘述。

3.1.2 流量信息概览[Summary]

顾名思义，流量信息概览是以图形和表单形式，对 NAM 监控的所有信息进行汇总，内容包括流量信息、主机信息、负载情况和流分布情况。

1. 流量汇总界面[Summary/Traffic]

流量汇总界面主要包括物理/逻辑接口的流量信息和各种协议的流量统计、报文统计等信息。

(1)　NAM 监控接口的信息

NAM监控的接口包括物理接口（eth0）和逻辑接口（如NetFlow-device.2），如图3-2所示。下方的饼图显示了各个接口流量所占的比重。

说明：

NAM 监控的物理接口的流量是 MSR 系列路由器 GE 接口的镜像流量。

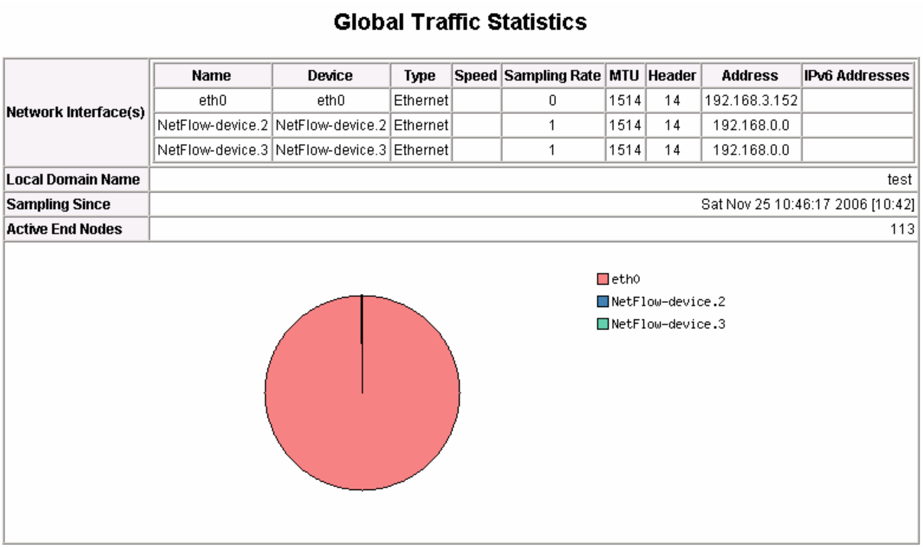
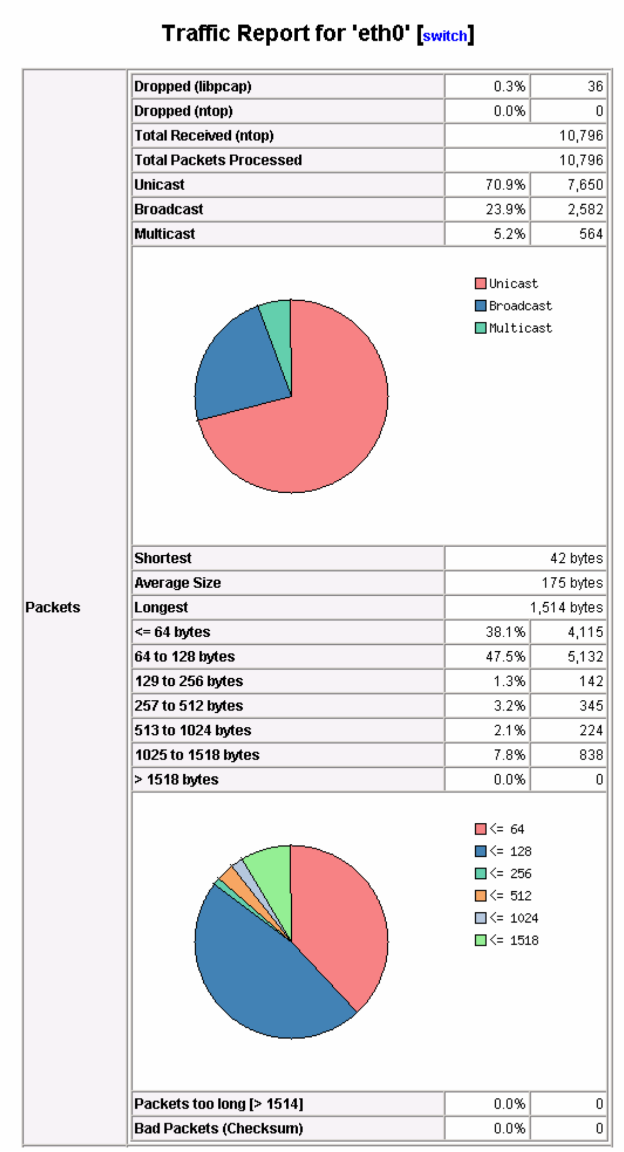


图3-2 Global Traffic Statistics

(2)　NAM 监控的具体接口的流量信息

对eth0 接口的报文统计方式包括报文的传输方式、报文的大小等如图 3-3所示。点击“switch”链接，可以查看其他接口的报文统计。



Traffic Report for 'eth0' [switch]

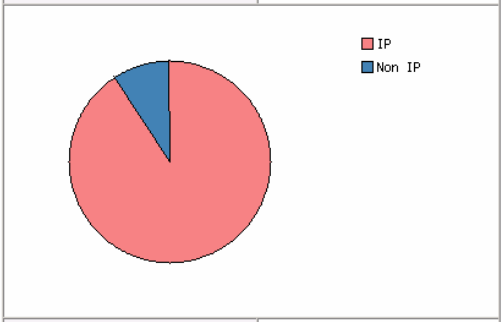
Packets	Dropped (libpcap)	0.3%	36
	Dropped (ntop)	0.0%	0
	Total Received (ntop)		10,796
	Total Packets Processed		10,796
	Unicast	70.9%	7,650
	Broadcast	23.9%	2,582
	Multicast	5.2%	564
	Shortest		42 bytes
	Average Size		175 bytes
	Longest		1,514 bytes
	<= 64 bytes	38.1%	4,115
	64 to 128 bytes	47.5%	5,132
	129 to 256 bytes	1.3%	142
	257 to 512 bytes	3.2%	345
	513 to 1024 bytes	2.1%	224
	1025 to 1518 bytes	7.8%	838
	> 1518 bytes	0.0%	0
	Packets too long [> 1514]	0.0%	0
	Bad Packets (Checksum)	0.0%	0

图3-3 eth0 接口的报文信息

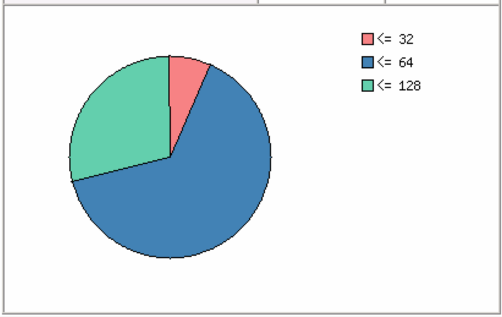
对eth0 接口的流量统计包括是否分片、TTL的范围、最近一段时间的流量等，如图 3-4所示。同时，点击可以查看历史信息，包括最近一年到最近一小时的历史记录。

Traffic

Total	2.1 MB [10,796 Pkts]
IP Traffic	1.9 MB [1.9 MB Pkts]
Fragmented IP Traffic	0 [0.0%]
Non IP Traffic	191.5 KB



Average TTL		64
TTL <= 32	5.2%	564
32 < TTL <= 64	49.4%	5,328
64 < TTL <= 96	0.0%	0
96 < TTL <= 128	22.1%	2,390
128 < TTL <= 160	0.0%	0
160 < TTL <= 192	0.0%	0
192 < TTL <= 224	0.0%	0
224 < TTL <= 256	0.0%	0



Network Load

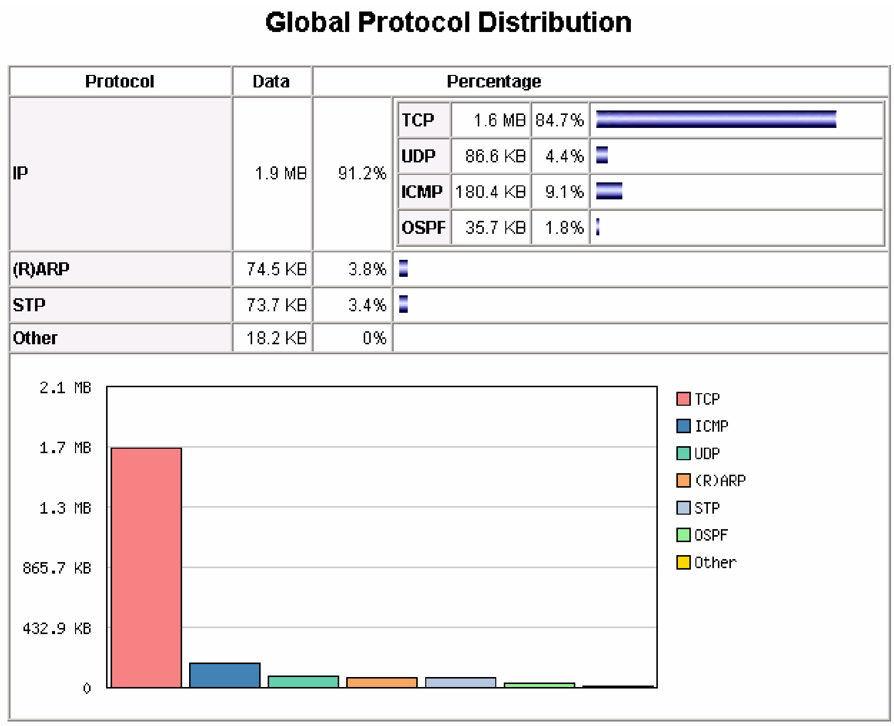
Actual	15.8 Kbps	13.0 Pkts/sec
Last Minute	8.4 Kbps	10.0 Pkts/sec
Last 5 Minutes	29.0 Kbps	17.3 Pkts/sec
Peak	160.7 Kbps	58.7 Pkts/sec
Average	27.7 Kbps	16.8 Pkts/sec

Historical Data

图3-4 eth0 接口的流量统计

(3) 协议的分布情况

NAM能对报文所使用的协议进行分类，如图 3-5所示。表格中具体的百分比和柱状图可以清晰的显示各种协议在总流量中所占的比重。



Global Protocol Distribution

Protocol	Data	Percentage				
IP	1.9 MB	91.2%	TCP	1.6 MB	84.7%	
			UDP	86.6 KB	4.4%	
			ICMP	180.4 KB	9.1%	
			OSPF	35.7 KB	1.8%	
(R)ARP	74.5 KB	3.8%				
STP	73.7 KB	3.4%				
Other	18.2 KB	0%				

图3-5 协议分布图

(4) 各种 TCP/UDP 协议的分布情况

NAM能细致的区分各种不同的TCP/UDP协议，在按照时间段分别进行统计（图 3-6）的同时，还使用了柱状图和表格进行汇总（图 3-7）。

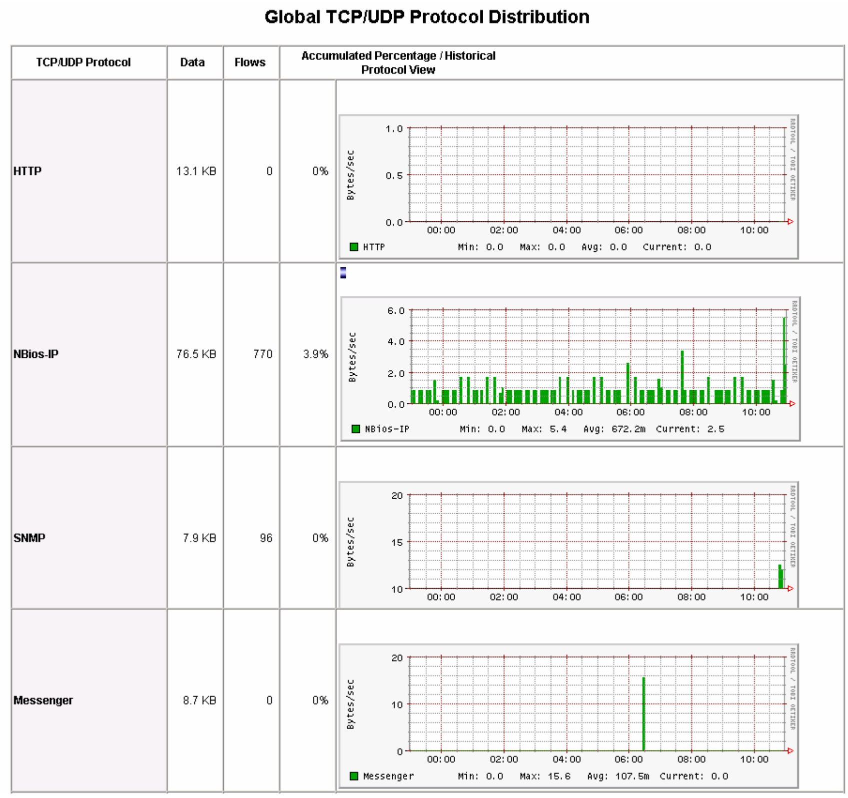


图3-6 TCP/UDP 协议的分布情况（1）

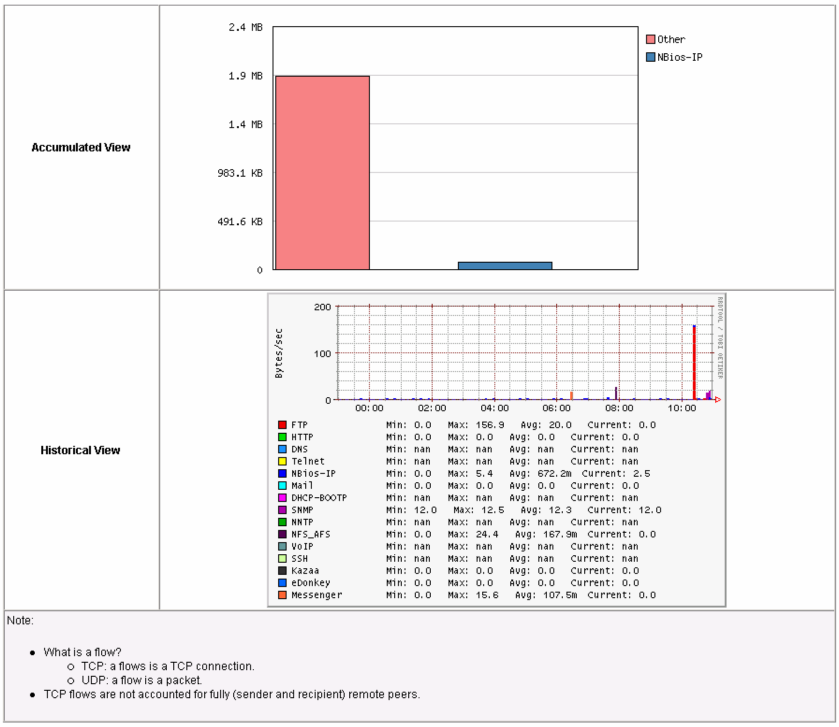


图3-7 TCP/UDP 协议的分布情况（2）

(5) 基于端口的 TCP/UDP 协议的分布情况

由于很多TCP/UDP协议采用非标准的端口进行通信，针对这种情况，NAM还对各种TCP/UDP协议的通信端口的分布情况进行了统计，如图 3-8所示。

TCP/UDP Traffic Port Distribution:
Last Minute View

TCP/UDP Port		Total	Sent	Rcvd
6003	6003	3.9 KB	2.0 KB	2.0 KB
6002	6002	3.9 KB	2.0 KB	2.0 KB
6001	6001	3.9 KB	2.0 KB	2.0 KB
x11	6000	3.9 KB	2.0 KB	2.0 KB
cvsup	5999	3.9 KB	2.0 KB	2.0 KB
5998	5998	3.9 KB	2.0 KB	2.0 KB
5997	5997	3.9 KB	2.0 KB	2.0 KB
5996	5996	3.9 KB	2.0 KB	2.0 KB
5995	5995	3.9 KB	2.0 KB	2.0 KB
5994	5994	3.9 KB	2.0 KB	2.0 KB
5993	5993	3.9 KB	2.0 KB	2.0 KB
5992	5992	3.9 KB	2.0 KB	2.0 KB
5991	5991	3.9 KB	2.0 KB	2.0 KB
5990	5990	3.9 KB	2.0 KB	2.0 KB
5989	5989	3.9 KB	2.0 KB	2.0 KB
5988	5988	3.9 KB	2.0 KB	2.0 KB
5987	5987	3.9 KB	2.0 KB	2.0 KB
5986	5986	3.9 KB	2.0 KB	2.0 KB
5985	5985	3.9 KB	2.0 KB	2.0 KB
5984	5984	3.9 KB	2.0 KB	2.0 KB
5983	5983	3.9 KB	2.0 KB	2.0 KB
5982	5982	3.9 KB	2.0 KB	2.0 KB
5981	5981	3.9 KB	2.0 KB	2.0 KB
5980	5980	3.9 KB	2.0 KB	2.0 KB
5979	5979	3.9 KB	2.0 KB	2.0 KB
5978	5978	3.9 KB	2.0 KB	2.0 KB
5977	5977	3.9 KB	2.0 KB	2.0 KB
5976	5976	3.9 KB	2.0 KB	2.0 KB
5975	5975	3.9 KB	2.0 KB	2.0 KB
5974	5974	3.9 KB	2.0 KB	2.0 KB
5973	5973	3.9 KB	2.0 KB	2.0 KB
5972	5972	3.9 KB	2.0 KB	2.0 KB

Notes:

- sum(total traffic per port) = 2*(total IP traffic) because the traffic per port is counted twice (sent and received)
- This report includes broadcast packets

图3-8 基于端口的 TCP/UDP 协议的分布情况

2. 网络中主机的信息[Summary/Hosts]

主机信息界面主要包括主机所在的域、IP地址、MAC地址、占用网络的带宽等基本信息，如图 3-9所示。通过左上角的Bytes/Packets链接，可以切换带宽的统计方式为按字节统计/按包数统计。显示带宽时，深绿色表示发送带宽，蓝色表示接收带宽。

Host Information

Traffic Unit: [Bytes] [Packets]

Host	Domain	IP Address	MAC Address	Other Name (s)	Bandwidth	Nw Board Vendor	Hops Distance	Host Contacts	Age/Inactivity		AS
198.19.1.2		198.19.1.2						1	10:41	1 sec	
192.168.0.200		192.168.0.200	00:05:5D:08:FE:B3			D-Link Systems, Inc.		7	10:43	0 sec	
bridge sp. tree/osi route:00:00:00			01:80:C2:00:00:00			Bridge Sp. Tree/OSI Route		2	10:42	0 sec	
192.168.1.57		192.168.1.57						1	10:31	1 sec	
huawei technologies co., ltd.:00:60:58			00:E0:FC:00:60:58			HUAWEI TECHNOLOGIES CO., LTD.		2	10:40	1 sec	
224.0.0.5		224.0.0.5				Multicast		7	10:38	2 sec	
laa (locally assigned address):65:43:79			12:34:56:65:43:79			LAA (Locally assigned address)		1	10:42	0 sec	
192.168.0.132		192.168.0.132	00:0F:E2:00:00:03			Hangzhou Huawei-3Com Tech. Co., Ltd.		1	10:15	3 sec	
192.168.0.60		192.168.0.60	00:E0:FC:00:AB:CD			HUAWEI TECHNOLOGIES CO., LTD.		4	10:07	3 sec	
laa (locally assigned address):00:42:49			FE:BC:00:00:42:49			LAA (Locally assigned address)		1	0 sec	3:38	
06:73:00:00:00:00			06:73:00:00:00:00					1	0 sec	4:18	
DC:33:00:00:42:49			DC:33:00:00:42:49					1	0 sec	7:27	
A8:C3:00:00:00:00			A8:C3:00:00:00:00					1	0 sec	9:46	
60:C0:00:00:42:49			60:C0:00:00:42:49					1	0 sec	9:50	
20:9F:00:00:42:49			20:9F:00:00:42:49					1	0 sec	10:18	
1.1.2.2		1.1.2.2						1	10:23	17 sec	
192.168.1.86		192.168.1.86						1	0 sec	4:47	
50:18:10:00:53:50			50:18:10:00:53:50					1	0 sec	20 sec	
50:18:10:00:82:2F			50:18:10:00:82:2F					1	0 sec	49 sec	
50:18:10:00:6D:CC			50:18:10:00:6D:CC					1	0 sec	53 sec	
50:18:10:00:AB:7C			50:18:10:00:AB:7C					1	0 sec	1:39	
50:18:10:00:1C:F3			50:18:10:00:1C:F3					1	0 sec	2:15	

图3-9 主机信息

3. 网络负载情况[Summary/Network Load]

网络负载情况显示图分别显示了最近十分钟、最近一小时、当天、以及最近一个月的网络负载，如图 3-10所示。

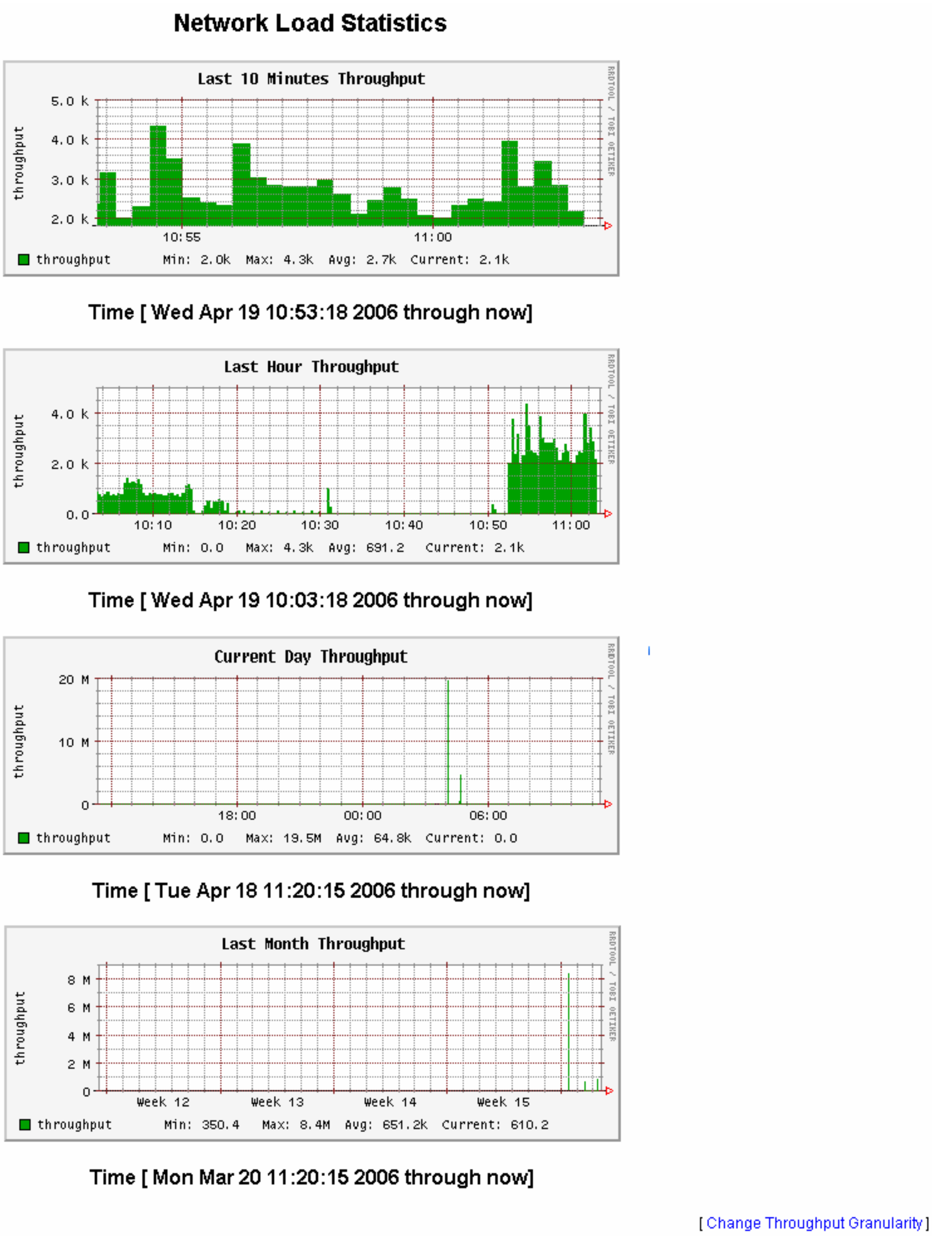


图3-10 网络负载情况

点击右下角的Change Throughput Granularity链接可以进入数据存储的参数设置界面，如图 3-11所示。具体可以设置数据存储间隔、数据更新间隔、数据导出地等参数。该界面和[Plugins/Round-Robin Databases/Configure]菜单项对应的RRD配置界面是同一个界面。

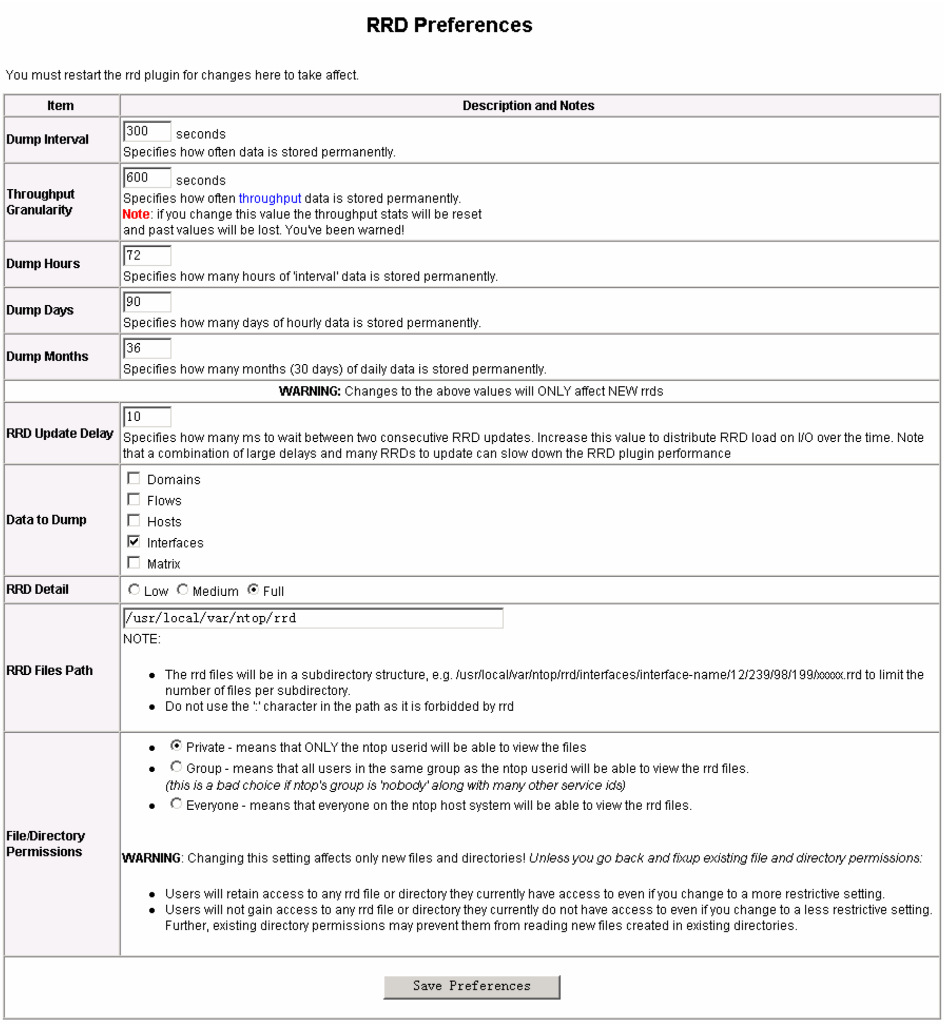
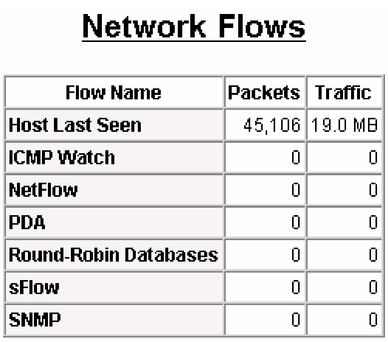


图3-11 存储参数的设置

4. 流的分布情况[Summary/Network Flows]

此界面主要显示了Host Last Seen插件和用户自定义的流规则的流量情况，如图3-12所示。



Network Flows

Flow Name	Packets	Traffic
Host Last Seen	45,106	19.0 MB
ICMP Watch	0	0
NetFlow	0	0
PDA	0	0
Round-Robin Databases	0	0
sFlow	0	0
SNMP	0	0

图3-12 流的分布情况

3.1.3 基础协议报表[All Protocols]

基础协议报表是以表单形式，给出基于主机和各种基础协议的流量报表，内容包括各种基础协议的流量统计、主机的流量统计和主机活动情况。

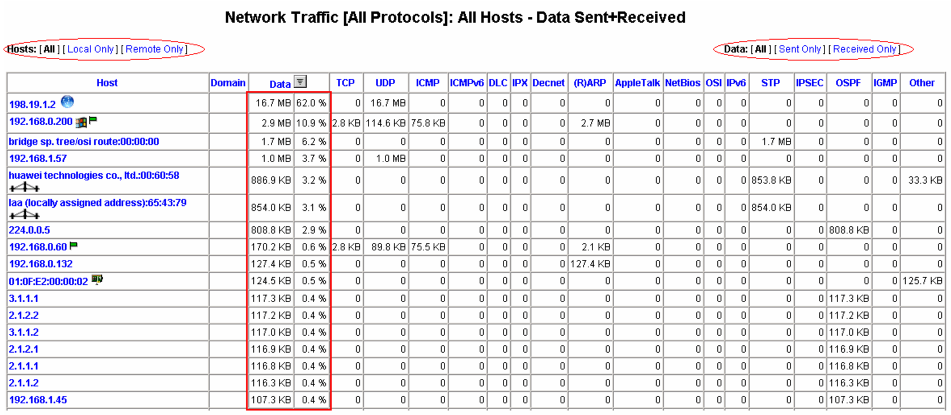
说明：

基础协议报表不对承载于TCP/UDP之上的各种协议进行细分。要了解这些协议的流量情况，可以查看3.1.4 1. (1)基于主机和IP协议的流量统计[IP/Summary/Traffic]。

1. 基于主机和协议类型的流量统计[All Protocols/Traffic]

此界面的流量是统计网络中具体主机的流量（包括总流量和各种协议的具体流量），这是和[Summary/Traffic]（3.1.2 1. 流量汇总界面[Summary/Traffic]）的主要区别。如图 3-13所示，每一台主机的总流量、所占的百分比、各种协议的流量都在表格中有所体现。

由于某些广播报文不包含特定的发送或接收主机的相关信息，因此界面中显示的流量可能并没有包含所有的广播报文，数据流量总和与[Summary/Traffic]中的 Global Protocol Distribution 也不一定相等。



Network Traffic [All Protocols]: All Hosts - Data Sent+Received

Hosts: [All] [Local Only] [Remote Only]

Data: [All] [Sent Only] [Received Only]

Host	Domain	Data		TCP	UDP	ICMP	ICMPv6	DLC	IPX	Decnet	(R)ARP	AppleTalk	NetBios	OSI	IPv6	STP	IPSEC	OSPF	IGMP	Other
198.19.1.2		16.7 MB	62.0 %	0	16.7 MB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.0.200		2.9 MB	10.9 %	2.8 KB	114.6 KB	75.8 KB	0	0	0	0	2.7 MB	0	0	0	0	0	0	0	0	0
bridge sp. tree/osi route:00:00:00		1.7 MB	6.2 %	0	0	0	0	0	0	0	0	0	0	0	0	1.7 MB	0	0	0	0
192.168.1.57		1.0 MB	3.7 %	0	1.0 MB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
huawei technologies co., ltd.:00:60:58		886.9 KB	3.2 %	0	0	0	0	0	0	0	0	0	0	0	0	853.8 KB	0	0	0	33.3 KB
laa (locally assigned address):65:43:79		854.0 KB	3.1 %	0	0	0	0	0	0	0	0	0	0	0	0	854.0 KB	0	0	0	0
224.0.0.5		808.8 KB	2.9 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	808.8 KB	0	0
192.168.0.60		170.2 KB	0.6 %	2.8 KB	89.8 KB	75.5 KB	0	0	0	0	2.1 KB	0	0	0	0	0	0	0	0	0
192.168.0.132		127.4 KB	0.5 %	0	0	0	0	0	0	0	127.4 KB	0	0	0	0	0	0	0	0	0
01:0F:E2:00:00:02		124.5 KB	0.5 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	125.7 KB
3.1.1.1		117.3 KB	0.4 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	117.3 KB	0	0
2.1.2.2		117.2 KB	0.4 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	117.2 KB	0	0
3.1.1.2		117.0 KB	0.4 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	117.0 KB	0	0
2.1.2.1		116.9 KB	0.4 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	116.9 KB	0	0
2.1.1.1		116.8 KB	0.4 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	116.8 KB	0	0
2.1.1.2		116.3 KB	0.4 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	116.3 KB	0	0
192.168.1.45		107.3 KB	0.4 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	107.3 KB	0	0

图3-13 全协议流量统计

2. 基于主机的流量的即时值和统计值[All Protocols/Throughput]

此界面主要显示主机流量和包数的即时值、平均值和最大值，如图 3-14所示。

Network Throughput: All Hosts - Data Sent+Received

Hosts: [All] [Local Only] [Remote Only]   Data: [All] [Sent Only] [Received Only]

Host	Domain	Data			Packets		
		Current	Avg	Peak	Current	Avg	Peak
1.1.2.2		22.9 bps	22.6 bps	147.4 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.2 Pkts/sec
2.1.1.1		65.6 bps	66.3 bps	472.0 bps	0.1 Pkts/sec	0.1 Pkts/sec	0.7 Pkts/sec
2.1.1.2		65.6 bps	66.1 bps	456.0 bps	0.1 Pkts/sec	0.1 Pkts/sec	0.7 Pkts/sec
2.1.2.1		78.7 bps	66.3 bps	472.0 bps	0.1 Pkts/sec	0.1 Pkts/sec	0.7 Pkts/sec
2.1.2.2		76.0 bps	66.5 bps	456.0 bps	0.1 Pkts/sec	0.1 Pkts/sec	0.7 Pkts/sec
3.1.1.1		78.7 bps	66.5 bps	472.0 bps	0.1 Pkts/sec	0.1 Pkts/sec	0.7 Pkts/sec
3.1.1.1		0.0 bps	0.1 bps	12.8 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.0 Pkts/sec
3.1.1.2		76.0 bps	66.3 bps	456.0 bps	0.1 Pkts/sec	0.1 Pkts/sec	0.7 Pkts/sec
192.167.0.11		0.0 bps	6.5 bps	336.0 bps	0.0 Pkts/sec	0.0 Pkts/sec	1.5 Pkts/sec
192.168.0.21		25.6 bps	25.0 bps	153.6 bps	0.1 Pkts/sec	0.1 Pkts/sec	0.4 Pkts/sec
192.168.0.33		0.0 bps	2.1 bps	257.6 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.2 Pkts/sec
192.168.0.60		102.7 bps	96.3 bps	739.2 bps	0.2 Pkts/sec	0.2 Pkts/sec	1.2 Pkts/sec
192.168.0.95		0.0 bps	0.1 bps	12.6 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.0 Pkts/sec
192.168.0.101		0.0 bps	0.1 bps	12.6 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.0 Pkts/sec
192.168.0.102		0.0 bps	0.1 bps	12.6 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.0 Pkts/sec
192.168.0.132		76.8 bps	71.7 bps	614.4 bps	0.2 Pkts/sec	0.2 Pkts/sec	1.6 Pkts/sec
192.168.0.158		0.0 bps	0.3 bps	34.3 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.0 Pkts/sec
192.168.0.159		0.0 bps	0.1 bps	12.8 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.0 Pkts/sec
192.168.0.198		23.2 bps	35.5 bps	510.4 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.5 Pkts/sec
192.168.0.199		0.0 bps	11.9 bps	250.9 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.3 Pkts/sec
192.168.0.200		1.8 Kbps	1.7 Kbps	13.9 Kbps	4.4 Pkts/sec	4.3 Pkts/sec	35.3 Pkts/sec
192.168.0.203		33.6 bps	1.0 bps	46.4 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.1 Pkts/sec
192.168.0.204		0.0 bps	0.3 bps	72.7 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.1 Pkts/sec
192.168.0.205		0.0 bps	14.6 bps	280.5 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.5 Pkts/sec
192.168.3.80		36.8 bps	16.5 bps	311.3 bps	0.1 Pkts/sec	0.0 Pkts/sec	0.6 Pkts/sec
192.168.0.217		0.0 bps	5.6 bps	128.0 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.3 Pkts/sec
192.168.0.231		0.0 bps	0.2 bps	12.8 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.0 Pkts/sec
192.168.0.250		0.0 bps	7.2 bps	132.8 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.2 Pkts/sec

图3-14 流量的即时值和统计值

3. 网络中主机的活动情况[All Protocols/Activity]

通过对主机在最近 24 小时中流量的统计和计算，可以确定主机最近 24 小时内流量分布的百分比，以此体现主机最活跃的时间段，如图 3-15所示。

在表格中用颜色表示特定时间段内主机的流量占最近 24 小时主机总流量的比重。不同的颜色表示的百分比不同，具体的颜色和百分比的对应关系可查看页面下方的说明。

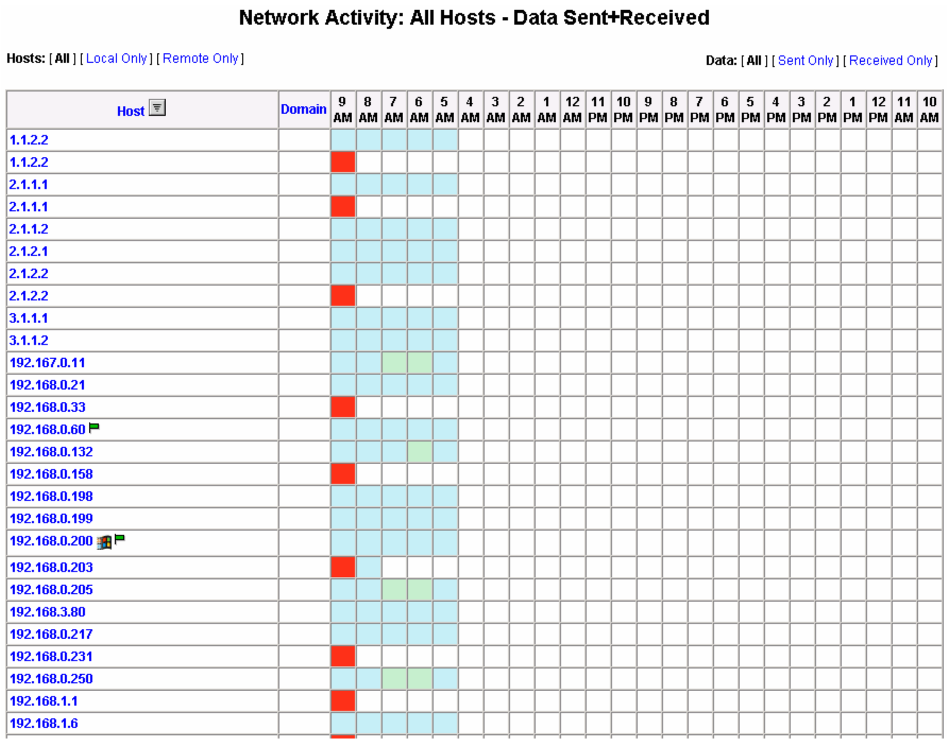


图3-15 主机的活动情况

3.1.4 IP 协议报表

IP 协议报表主要统计了承载于 TCP/UDP 之上的各种协议的流量、会话等相关信息。

1. IP 协议的信息汇总界面[IP/Summary]

IP 协议信息汇总包括：流量信息、组播信息、网段的具体信息、集群信息和本地/远程分布信息。

(1) 基于主机和 IP 协议的流量统计[IP/Summary/Traffic]

此界面主要是统计了网络中具体主机的流量（包括总流量和各种协议的具体流量）。协议都承载于TCP/UDP之上，这是和[All Protocol/Traffic]的主要区别。其中包括Internet上最常见的应用层协议HTTP和著名的P2P协议Bit Torrent，如图 3-16所示。

由于某些广播报文不包含特定的发送或接收主机的相关信息，因此界面中显示的流量可能并没有包含所有的广播报文，数据流量总和与[Summary/Traffic]中的 Global Protocol Distribution 也不一定相等。

Network Traffic [TCP/IP]: All Hosts - Data Sent+Received

Hosts: [All] [Local Only] [Remote Only]

VLAN: [1] [2] [All]

Data: [All] [Sent Only] [Received Only]

Host	Domain	Data		FTP	HTTP	DNS	Telnet	NBios-IP	Mail	DHCP-BOOTP	SNMP	NNTP	NFS/AFS	VoIP	X11	SSH	Gnutella	Kazaa	WinMX	DC++	eDonkey	BitTorrent	Messenger	Other IP
198.19.1.2 (vlan 2)		233.0 GB	100.0 %	47.8 MB	71.5 MB	23.8 MB	47.6 MB	71.2 MB	95.6 MB	47.8 MB	23.9 MB	24.0 MB	119.5 MB	47.6 MB	262.2 MB	24.0 MB	71.8 MB	23.9 MB	47.4 MB	0	119.3 MB	2.8 GB	166.6 MB	228.9 GB
192.168.3.162		13.8 MB	0.0 %	0	901	0	0	179.8 KB	10.3 KB	0	0	0	10.3 KB	2.5 KB	0	0	0	9.8 KB	0	0	3.8 KB	0	616	13.6 MB
192.168.0.200		6.4 MB	0.0 %	0	0	0	0	592.2 KB	0	0	5.4 MB	0	0	0	0	0	0	0	0	0	0	0	0	446.7 KB
224.0.0.0		5.4 MB	0.0 %	0	0	0	0	0	0	0	5.4 MB	0	0	0	0	0	0	0	0	0	0	0	0	0
224.0.0.5		3.8 MB	0.0 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3.8 MB
192.168.1.45		3.4 MB	0.0 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3.4 MB
192.168.3.152		2.0 MB	0.0 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	308	2.0 MB
192.168.1.32		1.6 MB	0.0 %	0	0	0	0	1.6 MB	0	1.1 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.1.57		1.1 MB	0.0 %	0	0	0	0	1.1 MB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1.7 KB
192.168.1.22		558.6 KB	0.0 %	0	0	0	0	558.6 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.1.19		30.5 KB	0.0 %	0	0	0	0	28.7 KB	0	1.8 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.1.61		18.5 KB	0.0 %	0	0	0	0	16.2 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2.3 KB
192.168.1.76		18.2 KB	0.0 %	0	0	0	0	9.2 KB	0	9.1 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.0.33		17.4 KB	0.0 %	0	0	0	0	17.4 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.1.25		16.6 KB	0.0 %	0	0	0	0	16.6 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.0.158		12.1 KB	0.0 %	0	0	0	0	12.1 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.1.36 (vlan 1)		10.9 KB	0.0 %	0	0	0	0	4.9 KB	0	6.0 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.1.63		9.7 KB	0.0 %	0	0	0	0	9.7 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

图3-16 基于 IP 的流量信息

(2) 组播流量统计[IP/Summary/Multicast]

此界面主要统计网络中组播的发送和接收情况，如图 3-17所示。同时把每个组播目的地址显示为一台主机，这样就可以看到每种组播应用的具体流量。

Multicast Statistics

Host	Domain	Pkts Sent	Data Sent	Pkts Rcvd	Data Rcvd
192.168.0.200		2,961	246.5 KB	0	0
192.168.1.45		1,950	151.1 KB	0	0
224.0.0.0		0	0	2,949	245.8 KB
224.0.0.5		0	0	1,950	151.1 KB
224.0.1.24		0	0	3	199

图3-17 组播流量统计

(3) 域信息统计[IP/Summary/Internet Domain]

Statistics for all Domains

Name	Domain	TCP/IP								ICMP			
		Total				TCP		UDP		IPv4		IPv6	
		Sent		Rcvd		Sent	Rcvd	Sent	Rcvd	Sent	Rcvd	Sent	Rcvd
hcom.com		6.5 KB	100.0%	10.1 KB	100.0%	6.0 KB	9.6 KB	0	0	296	370	0	0

图3-18 域信息统计

(4) 网段的信息统计[IP/Summary/Host Clusters]

通过在NAM中的配置，可以把网段定义为Cluster。此界面显示了网段的流量信息，如图 3-19所示。

Statistics for all clusters

Name	Domain	TCP/IP								ICMP			
		Total				TCP		UDP		IPv4		IPv6	
		Sent		Rcvd		Sent	Rcvd	Sent	Rcvd	Sent	Rcvd	Sent	Rcvd
Home		234.0 GB	100.0%	14.8 MB	100.0%	5.1 MB	14.7 MB	233.9 GB	0	2.1 MB	80.2 KB	0	0

NOTE: You can define host clusters in the ntop preferences. Please understand that a host cluster is an aggregated view of hosts known to ntop.

图3-19 未知主机信息统计

点击网段的名称“Home”，即可查看该网段中每个主机具体的TCP/IP和ICMP流量信息，如图 3-20所示。

Statistics for hosts in cluster *Home*

Name	Domain	TCP/IP								ICMP			
		Total				TCP		UDP		IPv4		IPv6	
		Sent		Rcvd		Sent	Rcvd	Sent	Rcvd	Sent	Rcvd	Sent	Rcvd
192.168.0.21		138	0.0%	0	0.0%	0	0	0	0	0	0	0	0
192.168.0.132 (vlan 1)		864	0.0%	0	0.0%	0	0	0	0	0	0	0	0
192.168.0.158		138	0.0%	0	0.0%	0	0	0	0	0	0	0	0
192.168.0.200 (vlan 1)		828	0.0%	0	0.0%	0	0	0	0	0	0	0	0
192.168.0.205 (vlan 1)		138	0.0%	0	0.0%	0	0	0	0	0	0	0	0
192.168.1.35		733	0.0%	0	0.0%	0	0	733	0	0	0	0	0
192.168.1.45		476	0.0%	0	0.0%	0	0	0	0	0	0	0	0
192.168.1.57		2.2 KB	0.0%	0	0.0%	0	0	2.2 KB	0	0	0	0	0
192.168.1.63 (vlan 1)		751	0.0%	0	0.0%	0	0	751	0	0	0	0	0
192.168.1.70		414	0.0%	0	0.0%	0	0	0	0	0	0	0	0
192.168.1.229		138	0.0%	0	0.0%	0	0	0	0	0	0	0	0
192.168.3.80 (vlan 1)		5.7 KB	0.0%	36.4 KB	1.1%	5.2 KB	34.9 KB	0	0	296	1.2 KB	0	0
192.168.3.100 (vlan 1)		552	0.0%	0	0.0%	0	0	0	0	0	0	0	0
192.168.3.152		3.0 MB	4.9%	333.3 KB	9.9%	3.0 MB	333.0 KB	0	0	1.2 KB	296	0	0
192.168.3.162		330.1 KB	0.5%	2.9 MB	89.0%	327.8 KB	2.9 MB	1020	0	0	0	0	0
198.19.1.2 (vlan 2)		56.7 MB	94.5%	0	0.0%	0	0	56.7 MB	0	0	0	0	0

NOTE: You can define host clusters in the ntop preferences. Please understand that a host cluster is an aggregated view of hosts known to ntop.

图3-20 网段内每台主机的流量信息

点击图 3-19或图 3-20说明文字中的preferences链接，进入Preference的配置界面，如图 3-21所示。

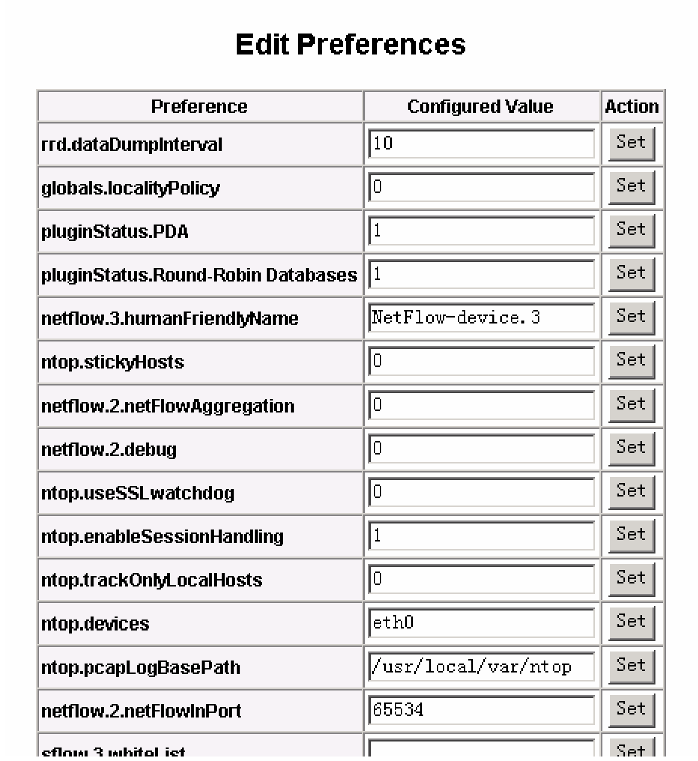


图3-21 Preferences 配置界面

在其中可以找到网段的配置，如图 3-22所示。

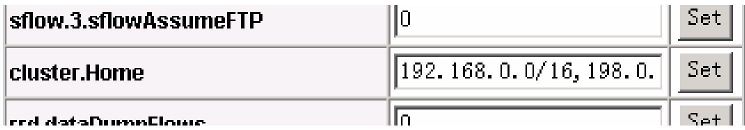


图3-22 已经配置好的网段

在界面最后的编辑框中可以定义新的网段，如图 3-23所示。图中定义了新的网段test。

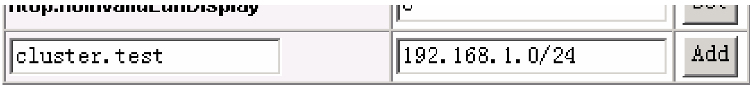


图3-23 定义新的网段

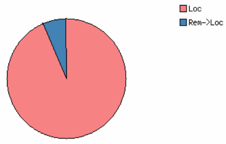
说明：

Preference 配置界面也可以通过[Admin/Configure/Preferences]进入。

(5) 本地/远程流量的全局分布[IP/Summary/Distribution]

此界面统计了本地、本地到远程、远程到本地、远程到远程的流量信息，如图 3-24所示。界面上方的饼图显示了比例，其他表单显示了具体数据。

IP Protocol Distribution



Local Traffic

IP Protocol	Data	Percentage
TCP vs. UDP	2.9 MB	TCP 100 % UDP 0 %

TCP/UDP Protocol	Data	Percentage	
NBios-IP	0.5 KB	0%	
Other TCP/UDP-based Protocols	2.9 MB	100.0%	

Remote to Local Traffic

IP Protocol	Data	Percentage
TCP vs. UDP	195.5 KB	TCP 0 % UDP 100 %

TCP/UDP Protocol	Data	Percentage	
NBios-IP	194.1 KB	99.3%	
Other TCP/UDP-based Protocols	1.4 KB	0%	

Remote Traffic

IP Protocol	Data	Percentage
TCP vs. UDP	36.9 KB	TCP 0 % UDP 100 %

TCP/UDP Protocol	Data	Percentage	
FTP	0.4 KB	0%	
HTTP	0.2 KB	0%	
DNS	0.2 KB	0%	
Telnet	0.2 KB	0%	
Mail	0.2 KB	0%	
DHCP-BOOTP	0.4 KB	0%	
SNMP	19.5 KB	52.8%	
SSH	0.2 KB	0%	
Other TCP/UDP-based Protocols	15.8 KB	42.9%	

Local to Remote Traffic

No Data To Display (yet)

图3-24 本地/远程流量的全局分布图

说明：

- 本地/远程流量全局分布界面并没有给出具体主机的流量信息，这部分信息请参见 2. 基于主机的本地/远程流量分布。
- 区分本地和远程的相关说明，请参见第 4 章 12. NAM中的local和remote是怎么定义的？

---

2. 基于主机的本地/远程流量分布

NAM 把 IP 流量划分成四种：本地、本地到远程、远程到本地和远程到远程。四种情况的统计界面类似，以下仅以本地流量为例进行说明。

如图 3-25所示，界面显示了本地主机之间通信的IP流量统计信息。

Local IP Traffic

Host	IP Address	Data Sent		Data Rcvd	
192.168.0.207 (Vlan 1)	192.168.3.80	6.4 KB	1.2 %	42.6 KB	7.9 %
192.168.3.152	192.168.3.152	488.2 KB	90.9 %	48.7 KB	9.1 %
192.168.3.162	192.168.3.162	42.4 KB	7.9 %	445.5 KB	83.0 %

Total Traffic	Data Sent	Data Rcvd	Used Bandwidth
536.9 KB	536.9 KB	536.9 KB	24.0 bps

图3-25 本地流量

3. 本地主机的具体情况

NAM 对本地主机进行统计和分析，以表单形式给出了本地主机的 TCP/UDP 端口使用、TCP/UDP 会话、操作系统、提供的服务、本地子网的流量情况等信息。

(1) TCP/UDP 端口使用[IP/Local/Ports Used]

TCP/UDP: Local Protocol Usage

Reporting on actual traffic for 11 host(s) on 1 service port(s)

Service		Clients	Servers
telnet	23	• xiaohui	• 192.168.0.152

图3-26 TCP/UDP 端口使用情况

(2) 活动的 TCP/UDP 会话[IP/Local/Active TCP/UDP Sessions]

NAM对当前活动的TCP/UDP会话进行统计，主要包括会话双方的IP地址、端口号、接收和发送的数据量、会话建立和活动的一些基本信息，如图 3-27所示。

Active TCP/UDP Sessions

Client	Server	Data Sent	Data Rcvd	Active Since	Last Seen	Duration	Inactive	Latency	Note
192.168.0.207 :2752	192.168.3.152 :3000	1.0 KB	1.1 KB	Mon Nov 27 13:52:06 2006	Mon Nov 27 13:52:06 2006	0 sec	0 sec		
192.168.3.152 :3000	192.168.3.162 :2845	120	0	Mon Nov 27 13:49:39 2006	Mon Nov 27 13:49:39 2006	0 sec	2:27		
192.168.3.152 :3000	192.168.3.162 :2853	120	0	Mon Nov 27 13:49:40 2006	Mon Nov 27 13:49:40 2006	0 sec	2:26		
192.168.3.152 :3000	192.168.3.162 :2854	120	0	Mon Nov 27 13:49:40 2006	Mon Nov 27 13:49:40 2006	0 sec	2:26		
192.168.3.152 :3000	192.168.3.162 :2856	120	0	Mon Nov 27 13:49:40 2006	Mon Nov 27 13:49:40 2006	0 sec	2:26		
192.168.3.152 :3000	192.168.3.162 :2857	120	0	Mon Nov 27 13:49:40 2006	Mon Nov 27 13:49:40 2006	0 sec	2:26		
192.168.3.152 :3000	192.168.3.162 :2859	120	0	Mon Nov 27 13:49:40 2006	Mon Nov 27 13:49:40 2006	0 sec	2:26		
192.168.3.152 :3000	192.168.3.162 :2861	120	0	Mon Nov 27 13:49:40 2006	Mon Nov 27 13:49:40 2006	0 sec	2:26		
192.168.3.152 :3000	192.168.3.162 :2862	120	0	Mon Nov 27 13:49:43 2006	Mon Nov 27 13:49:43 2006	0 sec	2:23		
192.168.3.162 :2865	192.168.3.152 :3000	597	273	Mon Nov 27 13:49:43 2006	Mon Nov 27 13:49:43 2006	0 sec	2:23		
192.168.3.152 :3000	192.168.3.162 :2880	120	0	Mon Nov 27 13:49:45 2006	Mon Nov 27 13:49:45 2006	0 sec	2:21		
192.168.3.152 :3000	192.168.3.162 :2888	120	0	Mon Nov 27 13:49:46 2006	Mon Nov 27 13:49:46 2006	0 sec	2:20		
192.168.3.152 :3000	192.168.3.162 :2889	120	0	Mon Nov 27 13:49:46 2006	Mon Nov 27 13:49:46 2006	0 sec	2:20		
192.168.3.152 :3000	192.168.3.162 :2891	120	0	Mon Nov 27 13:49:46 2006	Mon Nov 27 13:49:46 2006	0 sec	2:20		
192.168.3.152 :3000	192.168.3.162 :2892	120	0	Mon Nov 27 13:49:46 2006	Mon Nov 27 13:49:46 2006	0 sec	2:20		
192.168.3.152 :3000	192.168.3.162 :2894	120	0	Mon Nov 27 13:49:46 2006	Mon Nov 27 13:49:46 2006	0 sec	2:20		
192.168.3.152 :3000	192.168.3.162 :2896	120	0	Mon Nov 27 13:49:46 2006	Mon Nov 27 13:49:46 2006	0 sec	2:20		
192.168.3.152 :3000	192.168.3.162 :2897	120	0	Mon Nov 27 13:49:46 2006	Mon Nov 27 13:49:46 2006	0 sec	2:20		
192.168.3.152 :3000	192.168.3.162 :2898	120	0	Mon Nov 27 13:49:47 2006	Mon Nov 27 13:49:47 2006	0 sec	2:19		
192.168.3.152 :3000	192.168.3.162 :2915	120	0	Mon Nov 27 13:49:47 2006	Mon Nov 27 13:49:47 2006	0 sec	2:19		
192.168.3.152 :3000	192.168.3.162 :2916	120	0	Mon Nov 27 13:49:47 2006	Mon Nov 27 13:49:47 2006	0 sec	2:19		

图3-27 活动的 TCP/UDP 会话

(3) 本地主机操作系统使用情况[IP/Local/Host Fingerprints]

此界面中显示了NAM收集的主机的相关信息。本地主机可以显示操作系统，远程主机不能显示操作系统；本地和远程主机的数量都将被统计，如图 3-28所示。

Local Host Fingerprints

OS Summary

Host	Windows 2000	Cisco 2851	Linux 2.4.xx
192.168.3.80 (vlan 1)	X		
00:13:80:A4:62:F9		X	
192.168.3.162	X		
192.168.3.152			X

OS	Total
Windows 2000	2
Cisco 2851	1
Linux 2.4.xx	1

Statistics

Scanned	
Hosts	119
Less:	
No fingerprint	115
Broadcast	0
Multicast	0
Remote	0
Non IP host	0
Gives:	
Possible to report	4
Less: Can not resolve*	0
Less: Unknown Fingerprint**	0

图3-28 本地主机操作系统信息

(4) 本地主机的角色[IP/Local/Hosts Characterization]

NAM可以识别本地主机在网络中提供的服务和其他一些特征，从而判断这些主机在网络中担当的角色。如图 3-29所示，角色还包括存在安全隐患的主机（包括MAC地址冲突、使用了 0 端口、连接的主机连超过 1024 等情况），以此提醒网络管理员需要重点注意。

Local Hosts Characterization

Host	Unhealthy Host	L2 Switch Bridge	Gateway	VoIP Host	Printer	NTP/DNS Server	SMTP/POP/IMAP Server	Directory/FTP/HTTP Server	DHCP/WINS Server	DHCP Client	P2P
huawei technologies co., ltd.:00:60:58		X									
192.168.3.80 (vlan 1)	X										
00:13:80:A4:62:F9			X								
laa (locally assigned address):65:43:79 (vlan 1)		X									
192.168.3.152	X										
Total	2 [6.2 %]	2	1								

图3-29 本地主机的角色

(5) 本地网络中主机间的连接图[IP/Local/Network Traffic Map]

NAM以示意图的方式显示了本地网络中的主机间的连接关系，如图 3-30所示。

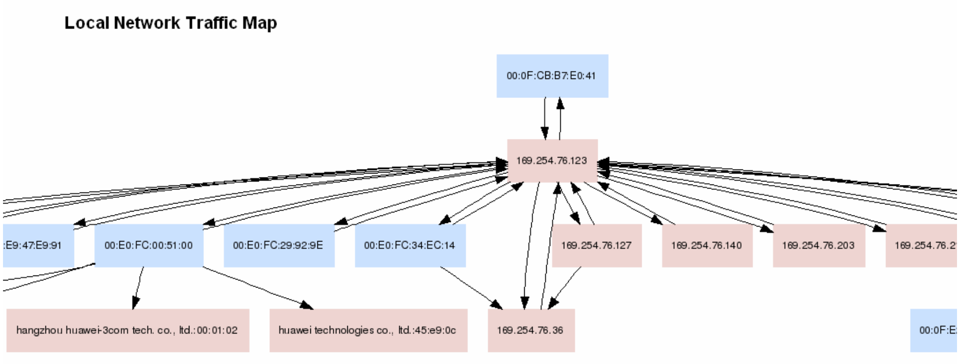


图3-30 本地网络中主机间的连接图

(6) IP 子网的流量信息[IP/Local/Ports Used]

NAM监控本地子网内主机之间的流量情况，以表单形式给出统计结果，如图 3-31所示。网络管理员可以根据这一信息从整体上监控本地子网内主机之间的数据交互情况。

IP Subnet Traffic Matrix

From \ To	192.168.3.80	192.168.3.152	192.168.3.162
192.168.3.80 (vlan 1)		296.0 KB	
192.168.3.152	296.0 KB		897.2 KB
192.168.3.162		897.2 KB	

图3-31 子网流量信息

3.2 典型应用

典型应用主要描述 NAM 及其插件在各个具体网络环境中的使用实例。主要包括三种类型的应用：

- 网络流量统计
- 网络流量监控
- 网络安全漏洞检测
- 网络优化和规划

说明：

本节旨在指导网络管理员使用 NAM，实例不覆盖所有 NAM 及其插件的功能。同时，描述过程中涉及的参数将不作具体说明。参数的具体说明请参见附录。

3.2.1 网络流量统计（一）NetFlow 流量分析

1. 网络环境

企业网中的流量分为两类：Intranet 和 Internet 进行通信的流量、Intranet 主机之间进行通信的流量。网络管理员对于这两类流量都很关心。路由器是企业网的出口，集成于路由器上的 NAM 能很方便的监控 Intranet 和 Internet 通信的流量。那 NAM 是否能实现对内容流量的监控呢？答案是肯定的。只需使用 NAM 中的 NetFlow 插件，即可实现上述功能。

首先，网络管理员需要在网络设备上启用 NetFlow 技术（一种流量采集技术）。NetFlow 可以统计接口上报文的源/目的 IP 地址，源/目的端口号以及报文大小等信息，并将这些信息组织成 Flow 格式。网络设备把 NetFlow 信息发送给启用了 NetFlow 插件的 NAM，NAM 就可以对这些信息进行存储和分析。

网络管理员只需在待监控的网络设备上启用 NetFlow，即可实现对流经该网络设备的流量进行监控和分析。这一方式突破了物理地域的限制，也无需在网络中布置多个流量监控软件，实现了一套 NAM 软件，监控整个网络的功能。

图 3-32为某企业的网络拓扑图，NAM集成于企业的出口路由器上。

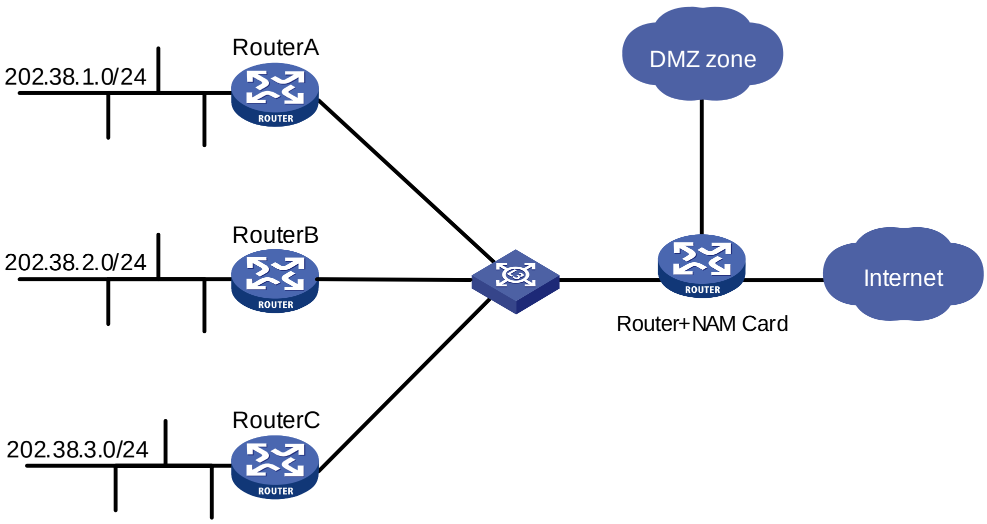


图3-32 NetFlow 流量分析组网图

2. 环境分析

如图 3-32所示，企业使用集成了NAM的路由器作为网络出口。内部网络主要有三个网段：202.38.1.0/24、202.38.2.0/24、202.38.3.0/24。

如果想监控这三个网段的流量，网络管理员只需进行如下两步操作：

(1) 在 MSR 系列路由器上启用 NAM，激活 NetFlow 插件。

(2) 在 RouterA、B、C 上分别启用 NetFlow 采集对应接口的流量。并设置发送 NetFlow 信息的目的 IP 为路由器的 Intranet 接口，即 202.38.4.2；目的端口为 65534。

这样 NAM 就能接收并存储这三个网络的流量信息，以便网络管理员直观的查看和分析。

3. 结果查看及分析

(1) 相关配置

NAM 提供 NetFlow 插件作为 NetFlow 分析工具，必须按照以下三个步骤进行正确的配置。

- 激活 NetFlow 插件

单击[Plugins/NetFlow/Active]菜单项，激活 NetFlow 插件。

说明：

若此菜单项显示为 Deactive，说明插件已经激活。

- 添加并配置 NetFlow 虚拟接口

单击[Plugins/NetFlow/Configure]菜单项，进入如图 3-33所示的界面。



图3-33 Plugins/NetFlow/Configure 界面

单击<Add NetFlow Device>按钮，即可创建NetFlow虚拟接口，并进入虚拟接口配置界面，如图 3-34所示。

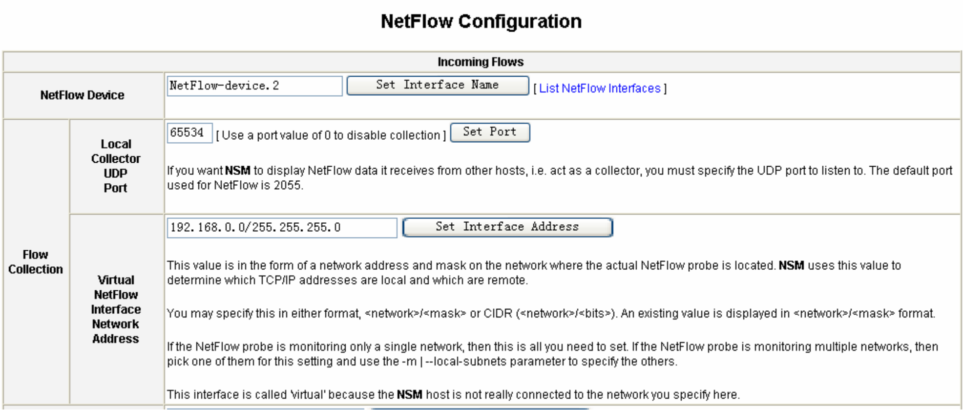


图3-34 NetFlow 接口配置界面

需要对参数进行如下配置：

NetFlow Device（interface name）：NetFlow

Local Collector UDP Port：65534

Virtual NetFlow Interface Network Address：202.38.0.0/16

其他参数均使用默认值。

- 切换网络接口

单击[Admin/Switch NIC]菜单项，进入如图 3-35所示的界面。把接口切换到NetFlow接口。

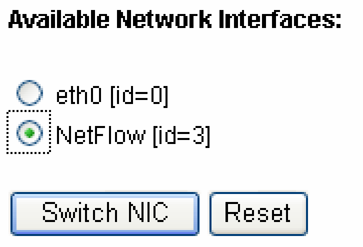
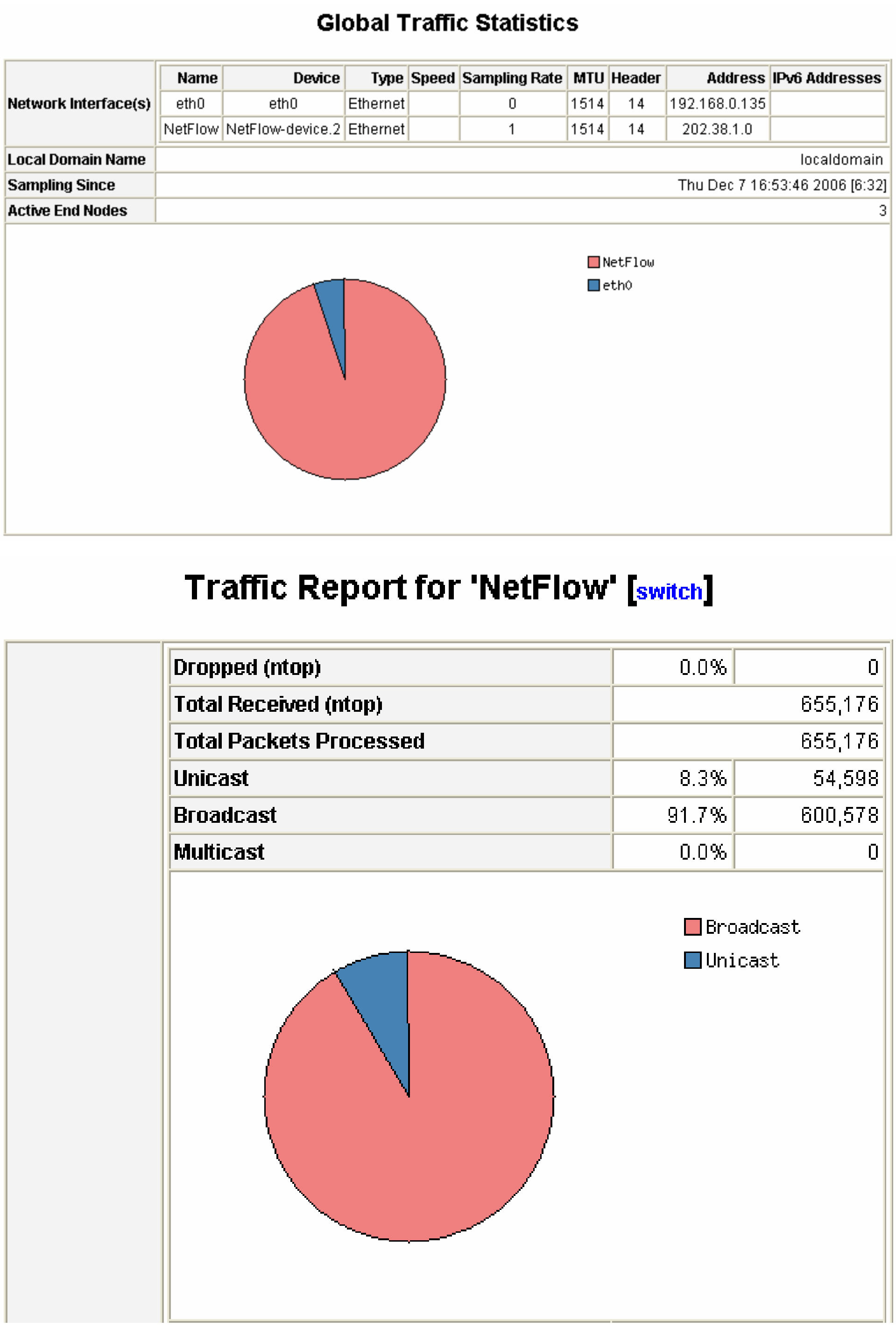


图3-35 切换接口界面

(2)　查看结果

上述配置完成后，等待一段时间，NAM 中即会形成最新的 NetFlow 流量信息。可以查看具体 NetFlow 数据的菜单包括 Summary、All Protocol 和 IP。

单击[Summary/Traffic]菜单项，进入如图 3-36所示的界面。可以查看NetFlow采集点（即启用了NetFlow的网络设备）的总流量信息。



Global Traffic Statistics

Network Interface(s)	Name	Device	Type	Speed	Sampling Rate	MTU	Header	Address	IPv6 Addresses
	eth0	eth0	Ethernet		0	1514	14	192.168.0.135	
	NetFlow	NetFlow-device.2	Ethernet		1	1514	14	202.38.1.0	

Local Domain Name	localdomain
Sampling Since	Thu Dec 7 16:53:46 2006 [6:32]
Active End Nodes	3

Traffic Report for 'NetFlow' [switch]

Dropped (ntop)	0.0%	0
Total Received (ntop)		655,176
Total Packets Processed		655,176
Unicast	8.3%	54,598
Broadcast	91.7%	600,578
Multicast	0.0%	0

图3-36 NetFlow 采集点总体流量信息（部分）

单击[Summary/Host]菜单项，进入如图 3-37所示的界面。可以查看NetFlow采集点统计的主机信息。

Host Information

Traffic Unit: [Bytes] [Packets]

Host	Domain	IP Address	MAC Address	Other Name(s)	Bandwidth
202.38.1.1		202.38.1.1			
202.38.1.5		202.38.1.5			
202.38.1.2		202.38.1.2			
202.38.1.14		202.38.1.14			
202.38.1.8		202.38.1.8			
202.38.1.11		202.38.1.11			
202.38.1.26		202.38.1.26			
202.38.1.20		202.38.1.20			
202.38.1.23		202.38.1.23			
202.38.1.17		202.38.1.17			
202.38.1.29		202.38.1.29			
202.38.1.32		202.38.1.32			

图3-37 主机统计信息

4. 注意事项

在配置 NetFlow 参数时，Local Collector UDP Port 一定要配置为正确的端口，否则 NetFlow 插件无法正常接收 NetFlow 数据。

3.2.2 网络流量统计（二）利用 RRD 查看历史流量图

1. 组网环境

在企业网中，各种网络异常情况发生在各个时间段中。网络管理员可以实时查看网络流量来定位分析各种异常情况，也需要通过查看历史数据来定位分析问题。同时，历史数据可以直观的反映网络使用情况的趋势和各种网络应用的分布，有助于网络管理员对网络进行综合评价。

NAM 的 RRD 插件可以存储全局的历史流量，结合 NAM 本身直观的图表显示功能，正好满足了网络管理员查看历史数据的需求。

图 3-38为某企业的网络拓扑图，安装了RRD插件的NAM集成于企业的出口MSR系列路由器上。网络管理员需要了解Intranet访问Internet占用的带宽，以及最近一段时间Intranet访问知名WEB站点 101.5.3.1 的流量。

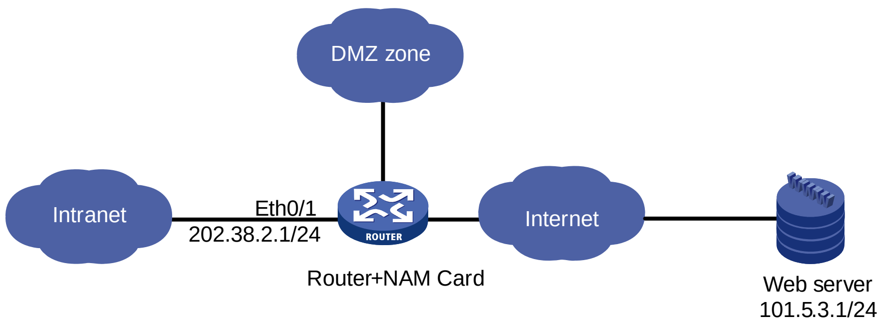


图3-38 查看 Intranet 服务器历史流量的组网图

2. 环境分析

根据 RRD 插件的特点，网络管理员只需启用并简单配置 NAM 中的 RRD 插件，就能对启用插件后的流量进行保存。网络管理员无需实时查看流量信息，只需每隔一段时间查看历史数据，即能了解企业 Intranet 访问 Internet 的带宽和访问特定站点的流量。

3. 结果查看及分析

(1) 相关配置

利用 RRD 查看流量图，需要进行一些必要的配置。

- 激活 RRD 插件

单击[Plugins/Round-Robin Database/Active]菜单项，激活 RRD 插件。

说明：

若此菜单项显示为 Deactive，说明插件已经激活。

- 配置 RRD 参数

单击[Plugins/ Round-Robin Database/Configure]菜单项，进入 RRD 插件的配置界面。RRD 插件的所有参数都有缺省值，本例中只需修改如下两个参数：

Dump Interval：向 RRD 增加一条记录的间隔，默认是 300 秒。间隔越小越能真实反映网络活动情况，同时增加 CPU 资源的消耗。设置此参数的值为 10 秒。

Data to Dump：指定需要存储到 RRD 的数据类型。缺省只保存 interfaces 的历史记录。为了查看访问 101.5.3.1 的流量，选中 Hosts。

- 重启 RRD 插件

重启 RRD 才能使新配置生效。单击[Plugins/Round-Robin Database/Deactive]菜单项关闭 RRD，然后再次激活 RRD 即可完成重启操作。

(2) 查看结果

NAM 中很多流量图都是由 RRD 导出的，通过这些流量图，即可查看相关的历史记录。同时，NAM 还提供专门的页面让用户根据自身的需要定制流量图。

- 查看 Intranet 访问 Internet 占用的带宽

一般情况下，Intranet的流量不会被镜像到路由器，所以流经路由器Eth0/1 接口的流量绝大部分都是Intranet访问Internet的流量。因此，网络管理员只需查看Eth0/1 接口上的吞吐量即可。单击[Summary/Network Load]菜单项，进入如图 3-39所示的界面，其中显示了过去十分钟和过去一小时。

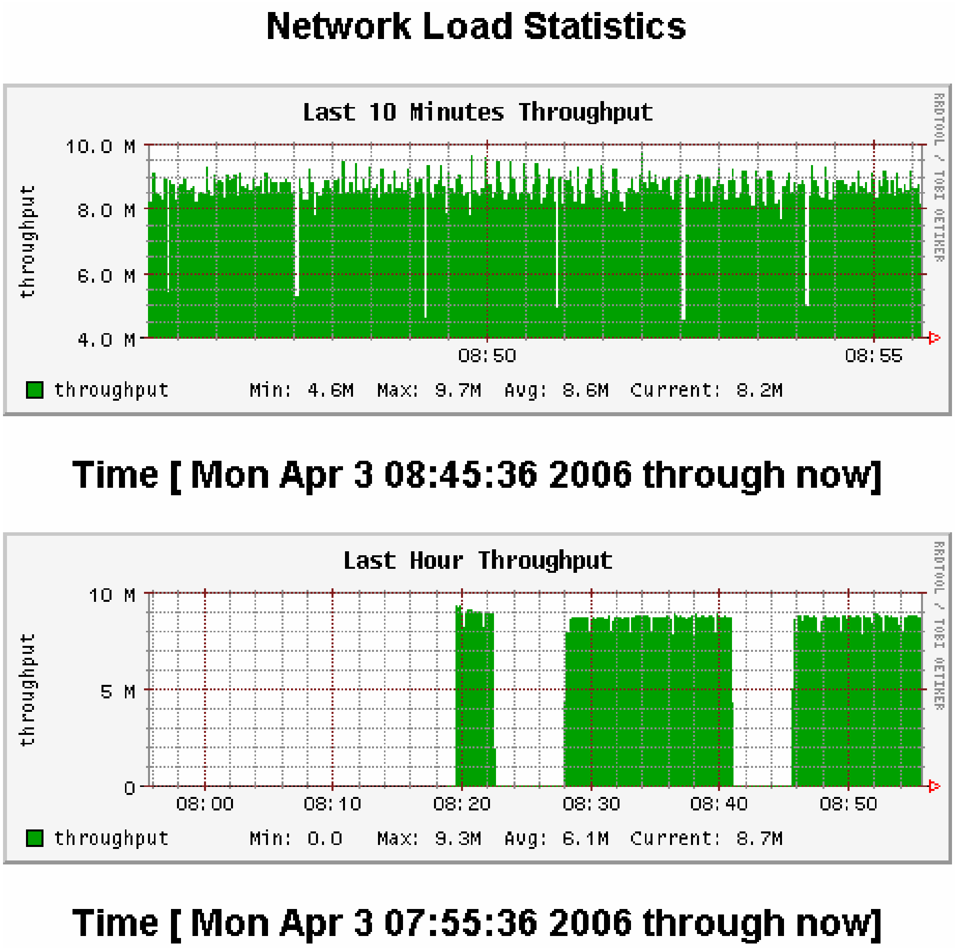


图3-39 网络负载流量图

说明：

根据 NAM 监控网络的时间和 RRD 参数的配置，界面中可能会显示过去一个月或一年的历史流量。

- 查看 Intranet 访问站点 101.5.3.1 的流量

单击[Plugins/Round-Robin Database/Arbitrary Graphs]菜单项，进入导出流量图界面。修改以下参数的值：

File： HTTP Sent Bytes

Host IP Address： 101.5.3.1

Legend：bytes

Title to appear above the graph：http of 101.5.3.1

Start：now

End：now-12h

配置完参数以后，单击<Make Request>按钮，生成流量图。该流量图体现过去十二小时 Intranet 访问 101.5.3.1 的 HTTP 流量。

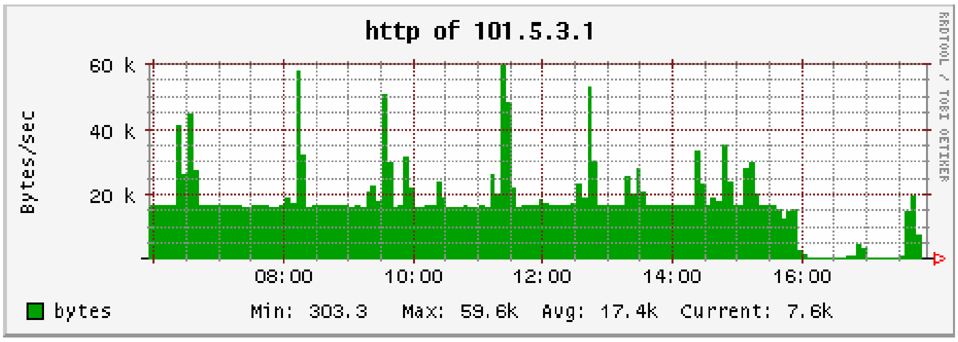


图3-40 HTTP 历史流量图

4. 注意事项

单击[Plugins/Round-Robin Database/Arbitrary Graphs]菜单项，进入导出流量图界面后，如果设置的File参数没有对应的RRD文件，则单击<Make Request>按钮生成流量图时，会报错，如图 3-41所示。



图3-41 出错页面

3.2.3 网络流量统计（三）支持对用户的 P2P 流量进行分析

1. 网络环境

随着人们越来越热衷于使用互联网，各种网络技术和网络服务满足了不同人群的各种需求。P2P 技术是近来比较流行的一种技术。这种技术提高了用户的下载速度，但是也占用了大量的带宽。网络管理员希望发现和监控网络中的 P2P 流量，以便在适当的时候采取必要的措施。

NAM 具备了在诸多网络流量中分辨各种应用层流量的能力，并通过人性化的图表显示了网络流量的统计结果。因此网络管理员使用 NAM 即可发现和监控 P2P 流量。。

图 3-42为某企业的网络拓扑图，NAM集成于企业的出口路由器上。近来，企业内部员工反映上网速度很慢，还经常掉线。网络管理员经过初步判断，认为企业内部有人使用P2P软件下载，占用了大量带宽。网络管理员将使用NAM软件对这一情况进行监控和分析。

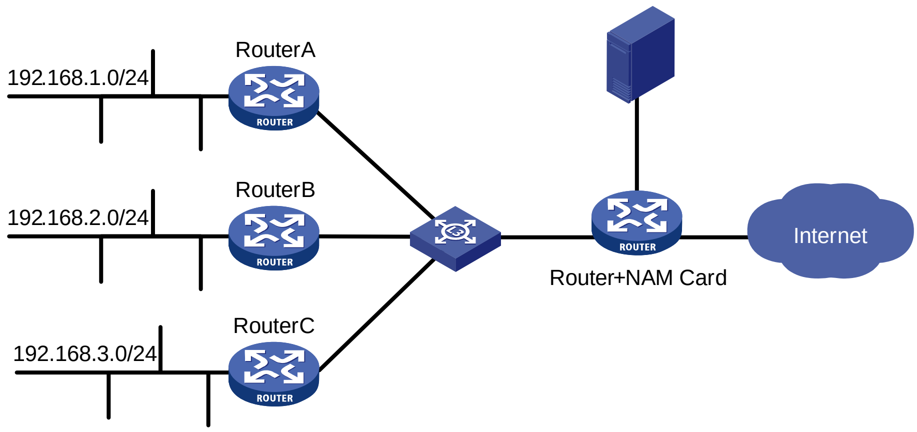


图3-42 P2P 流量分析组网图

2. 环境分析

如图 3-42所示，企业使用路由器连接Intranet和Internet。Intranet主要由三个网段组成：192.168.1.0/24、192.168.2.0/24、192.168.3.0/24。为了同时监控Intranet内部的P2P流量，分别在RouterA，RouterB，RouterC上使用NetFlow采集流量，NetFlow目的端口为默认的 2055，目的IP为路由器的NAM的管理IP。

经过以上配置，网络管理员只需登录 NAM，即可查看 NAM 提供的流量统计图表，实现对网络中 P2P 流量的监控。

说明：

关于NAM中NetFlow插件的典型应用，请参见3.2.1 网络流量统计（一）NetFlow流量分析。

3. 结果查看及分析

(1) 相关配置

配置NetFlow插件。具体请参见3.2.1 网络流量统计（一）NetFlow流量分析。

(2) 查看结果

- 查看各种 P2P 协议的流量信息。

单击[Summary/Traffic]菜单项，进入流量汇总界面。在页面中直接查看Global TCP/UDP Protocol Distribution图表，如图 3-43和图 3-44所示。把其中的几种P2P协议所占的百分比相加，得出所有P2P协议所占流量的百分比为 24%。

说明：

NAM 可以分析的 P2P 软件包括：BitTorrent、Gnutella、Kazaa、WinMX、DirectConnect（DC++）和 eDonkey。

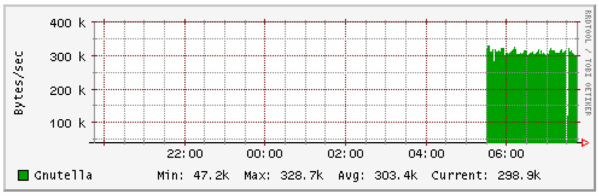
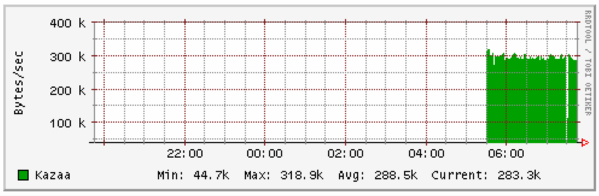
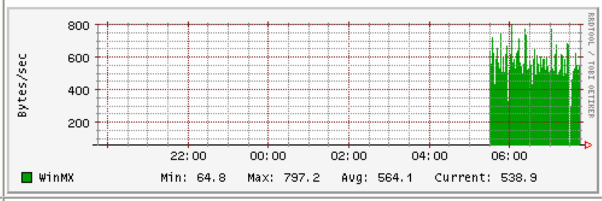
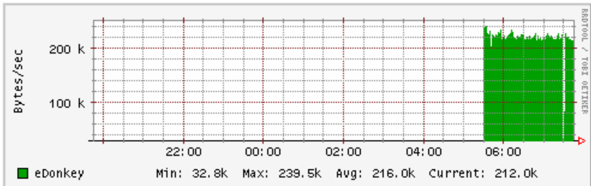
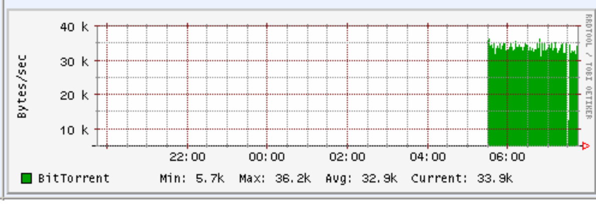
Gnutella	2.2 GB	2,406,573	9.0%	
Kazaa	2.1 GB	22,883,163	8.6%	
WinMX	4.3 MB	3,918	0%	
eDonkey	1.6 GB	1,711,273	6.4%	
BitTorrent	249.2 MB	228,128	0%	

图3-43 各种 P2P 协议所占流量的百分比

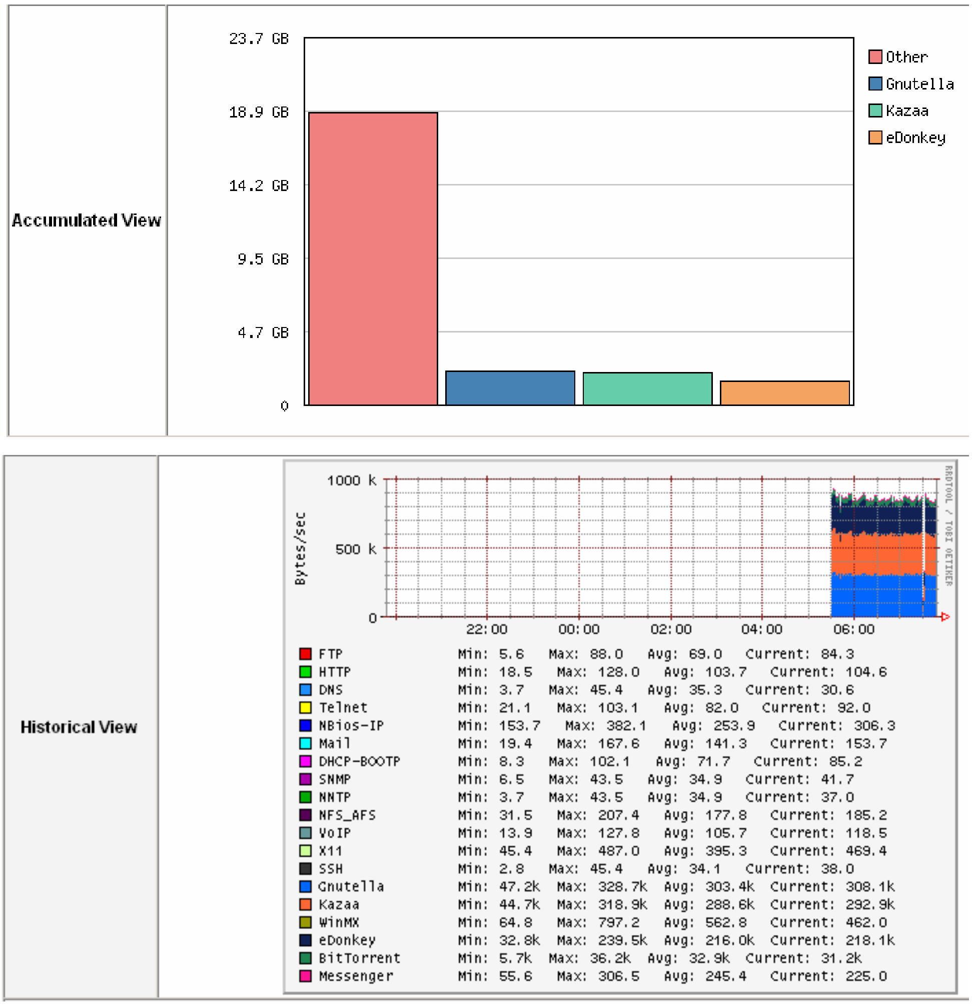


图3-44 各种 P2P 协议的比例图和历史信息

- 确定使用 P2P 软件的主机，并查看这些主机详细信息

单击[IP/Summary/traffic]菜单项，进入基于主机的IP流量统计界面。按照各种P2P协议排序，可以找到P2P流量较大的主机，如图 3-45和图 3-46所示。

Network Traffic [TCP/IP]: All Hosts - Data Sent+Received

Hosts: [All] [Local Only] [Remote Only]　　Data: [All] [Sent Only] [R

Host	Domain	Data		FTP	HTTP	DNS	Telnet	NBios-IP	Mail	X11	SSH	Gnutella
192.168.2.125		238.9 MB	5.2 %	0	0	0	0	0	0	0	0	238.9 MB
202.100.0.21		238.9 MB	5.2 %	0	0	0	0	0	0	0	0	238.9 MB
192.168.2.123		1.6 GB	35.6 %	43.9 KB	62.2 KB	22.5 KB	37.1 KB	65.5 KB	76.1 KB	238.5 KB	22.3 KB	66.2 KB
202.100.0.1		1.4 GB	30.6 %	43.9 KB	62.2 KB	22.5 KB	37.1 KB	65.5 KB	76.1 KB	238.5 KB	22.3 KB	66.2 KB

图3-45 按照 Gnutella 流量排序

Host	Domain	Data		FTP	Gnutella	Kazaa	WinMX	DC++	eDonkey	BitTorrent
192.168.2.123		2.0 GB	35.6 %	55.4 KB	82.8 KB	12.6 KB	651.1 KB	0	143.3 KB	36.5 MB
202.100.0.11		290.7 MB	5.0 %	0	0	0	594.7 KB	0	0	33.3 MB
202.100.0.1		1.7 GB	30.6 %	55.4 KB	82.8 KB	12.6 KB	56.3 KB	0	143.3 KB	3.3 MB
2.2.2.1		0	0.0 %	0	0	0	0	0	0	0

图3-46 按照BitTorrent流量排序

说明：

为了使图片更加清晰，图 3-45和图 3-46都做了一定裁减，让图片的信息更集中。

单击[All Protocols/Traffic]菜单项，进入如图 3-47所示的界面，即可查看P2P流量较大的主机占用带宽的情况。

Host	Domain	Data		TCP	UDP	ICMP	ICMPv6	DLC	IPX	Decnet	(R)ARP
192.168.2.123		2.7 GB	35.6 %	2.3 GB	386.3 MB	0	0	0	0	0	0
202.100.0.1		2.3 GB	30.6 %	2.3 GB	0	0	0	0	0	0	0
192.168.2.125		396.7 MB	5.2 %	0	396.7 MB	0	0	0	0	0	0
202.100.0.21		396.7 MB	5.2 %	0	396.7 MB	0	0	0	0	0	0
202.100.0.11		386.3 MB	5.0 %	0	386.3 MB	0	0	0	0	0	0
192.168.3.122		380.8 MB	5.0 %	0	380.8 MB	0	0	0	0	0	0
202.100.0.13		380.8 MB	5.0 %	0	380.8 MB	0	0	0	0	0	0
192.168.2.124		327.2 MB	4.3 %	0	327.2 MB	0	0	0	0	0	0
202.100.0.22		327.2 MB	4.3 %	0	327.2 MB	0	0	0	0	0	0

图3-47 主机流量所占总流量的百分比

点击Host列的主机IP，即可进入该IP对应的主机的详细信息显示界面，如图 3-48所示。

Info about 192.168.2.123

IP Address	192.168.2.123 [unicast] [Purge Asset]
First/Last Seen	Thu Apr 13 11:22:43 2006 - Thu Apr 13 11:35:55 2006 [Inactive since 0 sec]
Last MAC Address/Router	00:00:00:00:00:34
Host Location	Remote (outside specified/local subnet)
IP TTL (Time to Live)	64:64 [~0 hop(s)]
Total Data Sent	2.9 GB/27,357,415 Pkts/0 Retran. Pkts [0%]
Broadcast Pkts Sent	0 Pkts
Data Sent Stats	0 % / Rem 100 %
IP vs. Non-IP Sent	IP 100 % / Non-IP 0 %
Total Data Rcvd	0/0 Pkts/0 Retran. Pkts [0%]
Data Rcvd Stats	0 % / Rem 100 %
Sent vs. Rcvd Pkts	Sent 100 % / Rcvd 0 %
Sent vs. Rcvd Data	Sent 100 % / Rcvd 0 %
Historical Data	[ ]
Host Healthness (Risk Flags)	1. Traffic on suspicious IP ports

图3-48 主机详细信息显示界面

- 快速查看主机占用带宽的情况

如果网络管理员想快速查看哪些主机占用了大量带宽，可以使用NAM的PDA插件。单击[Plugins/PDA/View]菜单项，进入如图 3-49所示的界面。界面分别显示了接收和发送的流量排名前几位的主机（以IP方式显示）。

NSM for PDAs

Top Sending Hosts	Total
192.168.2.123	3.1 GB
192.168.2.125	466.6 MB
192.168.3.122	448.3 MB
192.168.2.124	385.0 MB
202.100.0.11	0

Top Receiving Hosts	Total
202.100.0.1	2.7 GB
202.100.0.21	466.6 MB
202.100.0.11	454.5 MB
202.100.0.13	448.3 MB
202.100.0.22	385.0 MB

Stats	Total
Sampling Time	27:35
Total	34,473,990
Unicast	34,473,989 [100.0%]
Broadcast	1 [0.0%]

图3-49 PDA 插件显示的流量排序界面

(3) 分析结果

通过上面的图表，网络管理员可以很清晰的指导使用 P2P 协议的主机主要为 192.168.2.123 和 192.168.2.125，同时占用了 20％以上的总带宽。

4. 建议网络管理员采取的措施

通过上述分析，网络管理员已经知道了使用 P2P 软件的主机、P2P 软件的类型及其使用的端口号。根据企业网具体情况，如果 P2P 软件的使用已经影响了正常的数据交互，建议网络管理员对路由器进行设置，关闭 P2P 软件使用的端口或配置 P2P 协议使用的带宽上限。

3.2.4 网络流量监控（一）网络错误配置

1. 网络环境

在企业网中，虽然网络管理员可以对网络中的主机进行统一的配置和部署，但是主机的使用者随时可以对主机进行相关修改，比如修改主机的 IP 地址，主机使用的 DNS 服务器地址等。一方面，使用者的随意修改可能使其无法正常使用网络；另一方面，各种修改使得网络管理员很难定位问题。NAM 可以帮助网络管理员解决以上烦恼。NAM 对网络进行实时监控，可以发现网络配置错误，使得网络管理员不用现场定位即可发现问题。

图 3-50为某企业的网络拓扑图，NAM集成于企业的出口路由器上。Intranet的网络设备把 192.168.0.0/24 网段的流量镜像到路由器上。Intranet的DNS服务器的地址为192.168.0.21。NAM实时监控网络，探察网络中的配置错误。

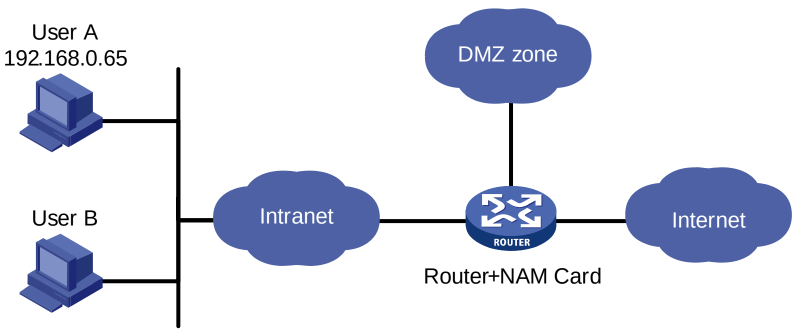


图3-50 网络配置错误组网图

2. 环境分析

NAM 实时监控 192.168.0.0/24 网段的流量，能发现 DNS 配置错误情况和重用 IP 地址的情况。

3. 结果查看及分析

常见的网络异常有以下几种，下文将使用 NAM 来一一定位。

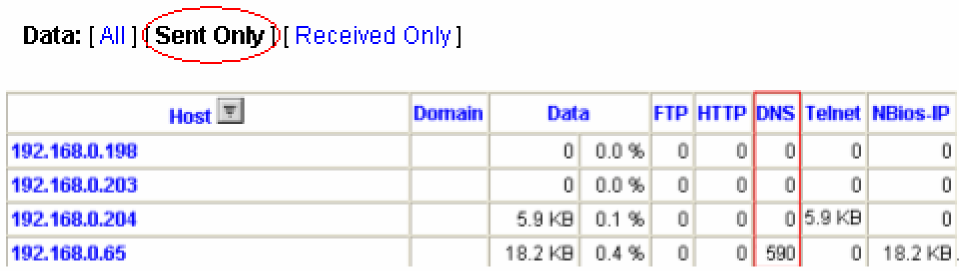
(1) 用户 A 造成访问 WEB 站点不成功

第一，使用 ping，查看用户 A 的网络连接是否存在问题。从用户 A ping DNS 服务器的地址，能 ping 通说明网络连接没有问题。

第二，判断 DNS 是否出现异常。如果用户 A 配置的 DNS 服务器有误，DNS 服务器就不会响应用户 A 的 DNS 报文。因此只需在 NAM 中是否有回应用户 A 的 DNS 报文。

NAM 提供基于主机的应用层流量的统计。单击[IP/Summary/Traffic]菜单项，进入查看具体协议报文的界面。

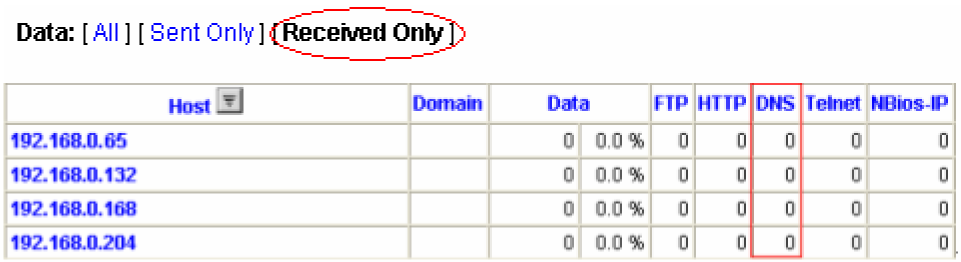
- 点击右上角的Sent Only链接，显示结果表明 192.168.0.65 发送了一定量的DNS报文，如图 3-51所示。



Host	Domain	Data		FTP	HTTP	DNS	Telnet	NBios-IP
192.168.0.198		0	0.0 %	0	0	0	0	0
192.168.0.203		0	0.0 %	0	0	0	0	0
192.168.0.204		5.9 KB	0.1 %	0	0	0	5.9 KB	0
192.168.0.65		18.2 KB	0.4 %	0	0	590	0	18.2 KB

图3-51 查看发送的 DNS 字节数

- 点击右上角的Received Only链接，结果表明 192.168.0.65 没有接受到DNS报文，如图 3-52所示。



Host	Domain	Data		FTP	HTTP	DNS	Telnet	NBios-IP
192.168.0.65		0	0.0 %	0	0	0	0	0
192.168.0.132		0	0.0 %	0	0	0	0	0
192.168.0.168		0	0.0 %	0	0	0	0	0
192.168.0.204		0	0.0 %	0	0	0	0	0

图3-52 查看接收的 DNS 字节数

192.168.0.65 的发送的 DNS 字节数为 590 字节，接收的 DNS 字节数为 0，说明用户 A 无法正常使用 DNS 服务，排除 DNS 服务器本身的问题后，网络管理员即可确定用户 A 的 DNS 服务器地址配置错误。

(2) 用户 B 将 IP 地址配置成了 192.168.0.65，与用户 A 的 IP 地址冲突。

NAM 可以记录 Intranet 主机的详细信息，包括 IP 地址，MAC 地址等。通过查看同一个 IP 地址是否存在不同的 MAC 来判断是否有 IP 地址冲突。

单击[Summary/Host]菜单项，进入如图 3-53所示的界面。其中显示了所有被NAM监控到的主机信息。点击主机列表的IP Adress项，使主机信息按照IP地址排列。

Host	Domain	IP Address	MAC Address
1.1.1.98		1.1.1.98	
lenovo-9637b2ca [NetBIOS]		3.3.3.1	
10.153.100.151		10.153.100.151	
192.168.0.1		192.168.0.1	00:E0:FC:29:4B:72
192.168.0.11		192.168.0.11	00:0D:88:F5:98:05
192.168.0.12		192.168.0.12	00:04:23:A7:5D:E5
192.168.0.21		192.168.0.21	00:E0:FC:50:12:24
192.168.0.22		192.168.0.22	00:E0:FC:2C:97:4C
192.168.0.65		192.168.0.65	00:E0:FC:00:12:35
gg[NetBIOS]		192.168.0.65	00:0D:88:F5:97:F0

图3-53 查看主机信息

很明显，IP 地址 192.168.0.65 对应了两个不同的 MAC 地址。由此判断网络中有两台主机的 IP 地址冲突。

4. 建议网络管理员采取的措施

通过上述分析，网络管理员已经知道了错误配置 DNS 和 IP 地址冲突的主机的 IP 地址。如果网络管理员保存了一份企业网设备信息的文档，立即就能定位到这些主机在企业网中的物理位置。之后，网络管理员即可采取相关的修复措施，如通知主机所有者修改错误配置等。

3.2.5 网络流量监控（二）网络服务器负载分析

1. 网络环境

因业务需要，很多企业经常在企业网内部或者向 Internet 提供一些网络服务（如 HTTP 服务、FTP 服务等）。为了保证这些网络服务能够正常被用户使用，并具备一定的稳定性和可靠性，这些服务器的管理员（往往也是企业的网络管理员）必须实时关注服务器是否运行正常。NAM 提供了对网络服务的数据收集功能，让网络管理员在 NAM 的界面中就能获悉各种网络服务的流量信息，以此来判断服务器的工作状态。

图 3-54为某企业的网络拓扑图，NAM集成于企业的出口路由器上。企业网中配备了HTTP服务器和FTP服务器，对企业网内部和Internet提供了HTTP服务和FTP服务。

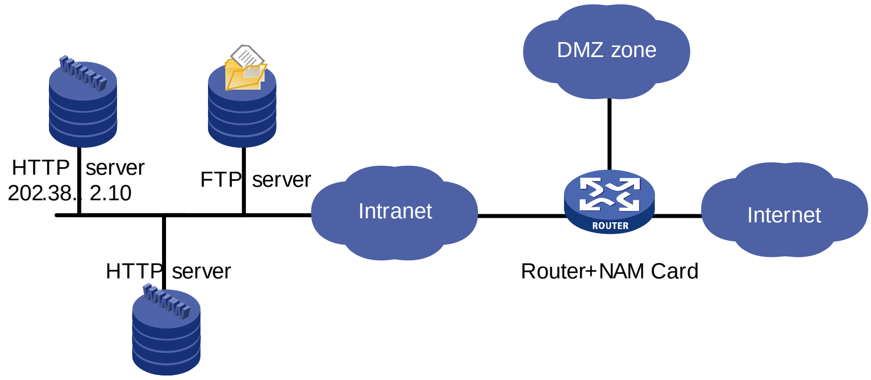


图3-54 网络服务器负载分析组网图

2. 环境分析

HTTP 服务器的 IP 地址为 202.38.2.10，网络管理员只需查看 HTTP 服务器的负载情况即可初步判断当前 HTTP 服务能否被正常使用。同时，查看 HTTP 服务器的历史流量，通过分析 HTTP 服务的流量分布，可以了解 HTTP 服务器的历史运行情况，有针对性的进行维护和管理。FTP 服务的判断方法类似。

3. 结果查看及分析

(1) 查看结果

- 查看 HTTP 服务器 202.38.2.10 每天的流量图，找出一天的流量规律。

单击[Plugins/ Round-Robin Database/Arbitrary Graphs]菜单项，进入 RRD 数据导出配置界面。修改以下参数的值：

File： bytesSend (byesRcvd)

Host IP Address： 202.38.2.10

Legend：bytes。

Title to appear above the graph：bytesSend of 202.38.2.10

Start：now

End：now-1d

Start 和 End 参数表明，导出的流量图以天为单位。

配置完参数以后，单击<Make Request>按钮，生成流量图。

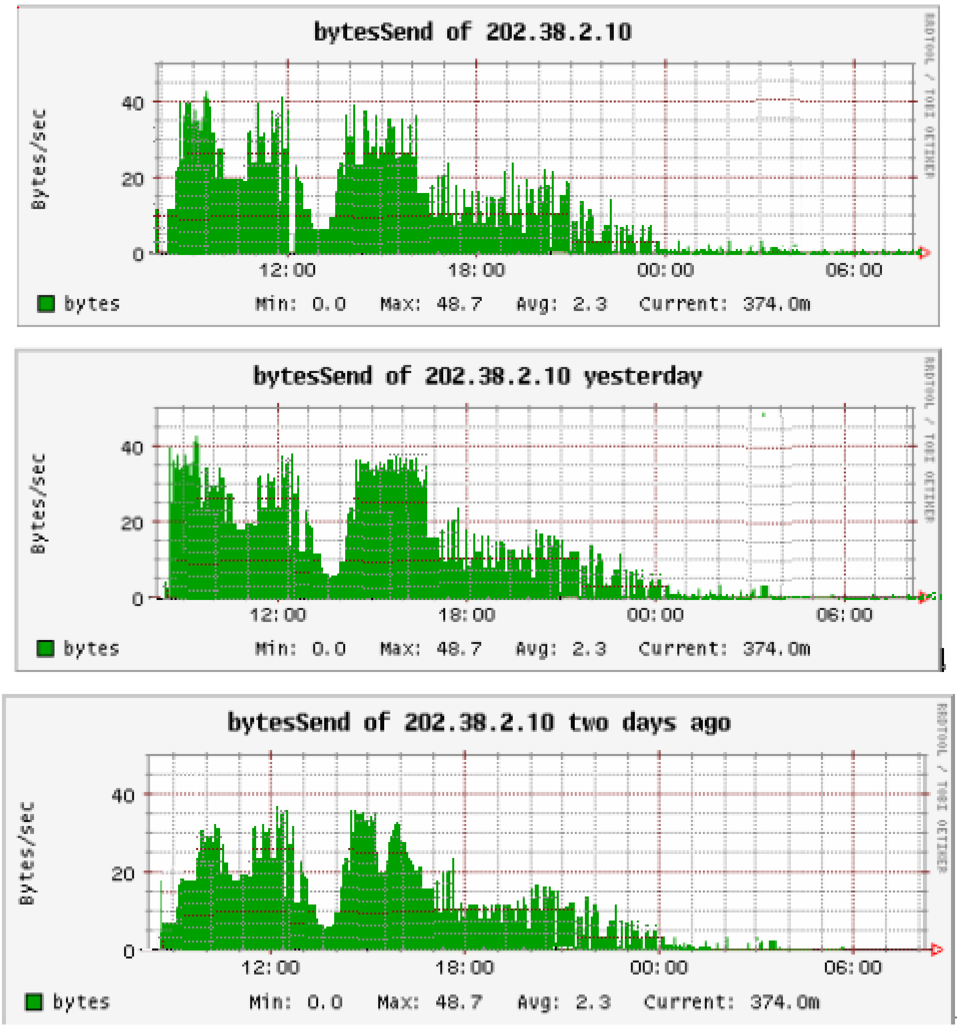


图3-55 网络服务器最近一天的流量图

上面三张图，分别是今天、昨天和前天的流量图，从图中可以推断出每天下午 3 点和上午 10 点左右 HTTP 服务器的流量比较大。

- 查看 HTTP 服务器 202.38.2.10 每周的流量图，找出一周的流量规律。

单击[Plugins/ Round-Robin Database/Arbitrary Graphs]菜单项，进入 RRD 数据导出配置界面。修改以下参数的值：

File： bytesSend (byesRcvd)

Host IP Address： 202.38.2.10

Legend：bytes。

Title to appear above the graph：bytesSend of 202.38.2.10 this week

Start：now

End：now-1w

Start 和 End 参数表明，导出的流量图以周为单位。

配置完参数以后，单击<Make Request>按钮，生成流量图。

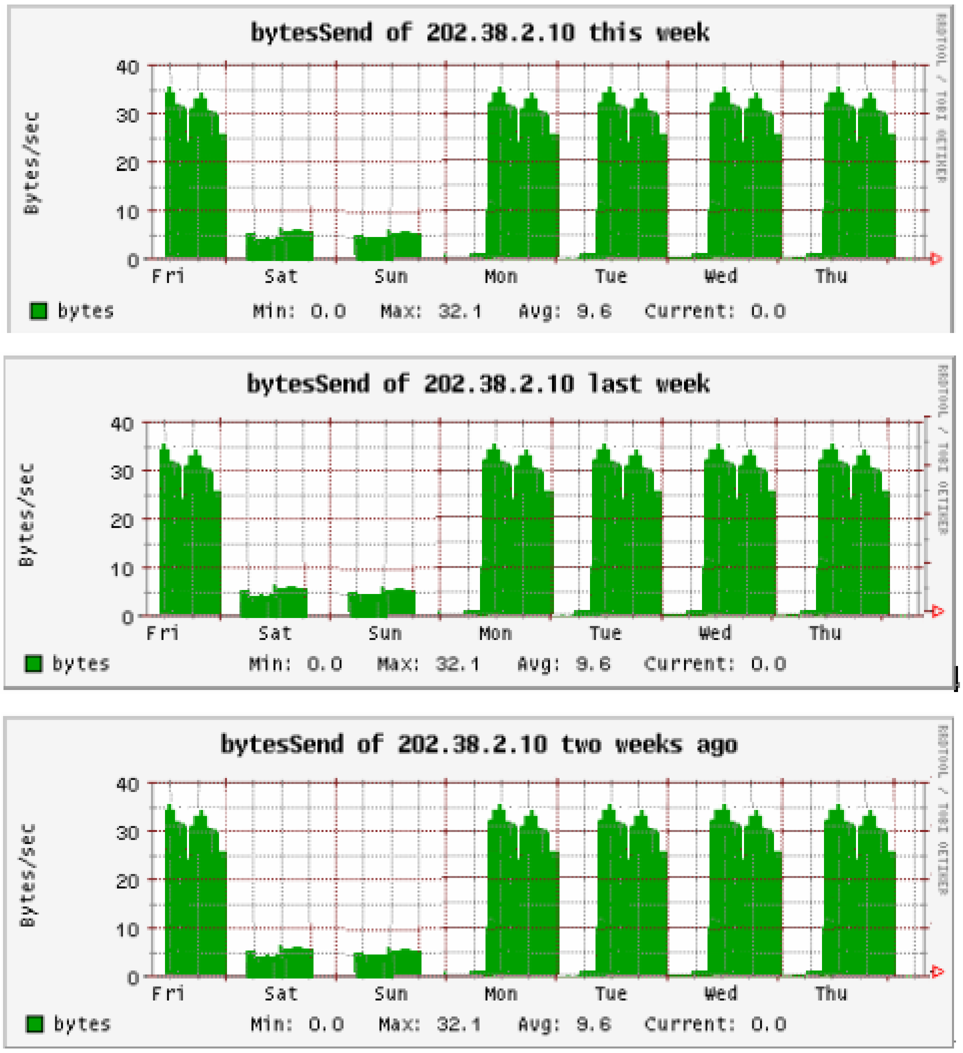


图3-56 网络服务器每周流量图

上面三张图，分别是本周、上周和上两周的流量图，从图中可以推断出周一到周五，HTTP 服务器的流量比较大，周末几乎无人使用 HTTP 服务。

- 查看 HTTP 服务器的 TCP 会话

单击[Summary/Hosts]菜单项，进入主机信息界面。点击 Host 202.38.2.10，显示 HTTP 服务器的具体信息。

Last Contacted Peers

Sent To	IP Address	Received From	IP Address
101.153.0.62	101.153.0.62	101.153.0.62	101.153.0.62
101.153.0.5	101.153.0.5	101.153.0.5	101.153.0.5
101.153.0.26	101.153.0.26	101.153.0.26	101.153.0.26
101.153.0.29	101.153.0.29	101.153.0.29	101.153.0.29
101.153.0.11	101.153.0.11	101.153.0.11	101.153.0.11
101.153.0.14	101.153.0.14	101.153.0.14	101.153.0.14
101.153.0.8	101.153.0.8	101.153.0.8	101.153.0.8
101.153.0.23	101.153.0.23	101.153.0.23	101.153.0.23
Total Contacts	5841	Total Contacts	5966

TCP/UDP Service/Port Usage

IP Service	Port	# Client Sess.	Last Client Peer	# Server Sess.	Last Server Peer
http	80			50374/9.2 MB	101.153.0.5

TCP/UDP Recently Used Ports

Client Port	Server Port
	• http

图3-57 近期访问 HTTP 服务器的主机

通过上图可以查看近期有哪些主机访问了 HTTP 服务器。

(2) 分析结果

通过查看 HTTP 服务器每天、每周的具体流量（特别是流量较大的时间段），可以分析 HTTP 服务器是否过载。上例的图中表明，HTTP 服务的流量较小，HTTP 服务器完全能满足现在的流量需求。

通过查看和 HTTP 服务器交互信息的主机 IP，可以分析是否有大量的 Internet 用户来访问 HTTP 服务器。上例的图中表明，并没有很多用户使用该企业网提供的 HTTP 服务，或者是因为宣传较少，或者是因为网站本身不吸引人。这些数据都可以作为参考数据。

3.2.6 网络安全漏洞检测（一）DOS 攻击检测

1. 组网需求

网络安全成为网络管理员越来越关注的问题。当网络中出现恶意攻击时，正确使用NAM，就能对几种常见的攻击行为进行检测和分析。

图 3-58为某企业的网络拓扑图，NAM集成于企业的出口路由器上。近来，企业内部员工反映访问企业内部的WEB服务器很慢，有时甚至无法访问。网络管理员将对这一情况进行排查和分析，其中使用了NAM来帮助定位问题。

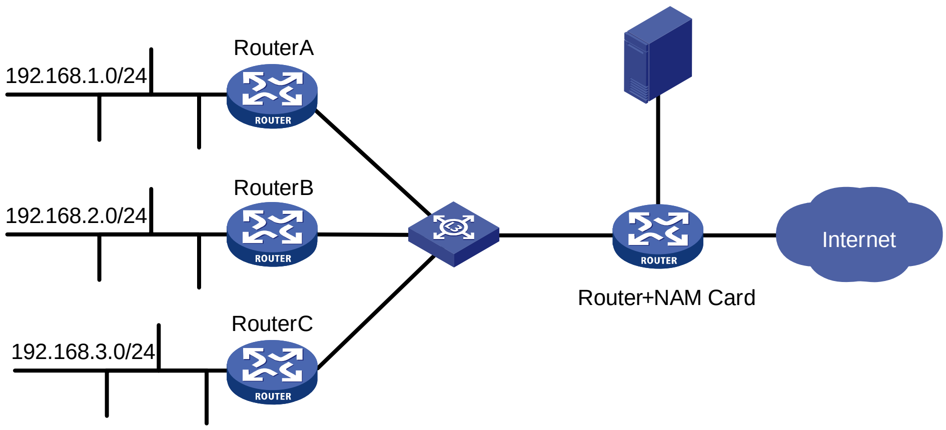


图3-58 DOS 攻击检测组网图

2. 环境分析

因为员工只是反映无法访问特定的服务器，而不是无法使用网络。因此初步判断大部分网络运行正常。在网络管理员的建议下，员工之间进行了主机互 ping 操作，发现 ping 正常，而员工的主机 ping 服务器时却丢包严重。初步判断为服务器存在问题。

为了进行细致而深入的分析，网络管理员使用NAM对服务器进行监控。在如图 3-58所示的组网环境中，网络管理员可以把服务器的流量镜像到NAM（集成于MSR系列路由器上）。登录NAM之后，通过查看NAM提供的流量统计图表，即可对服务器的流量进行监控，进而分析服务器的问题所在。

3. 结果查看及分析

(1) 查看结果

- 查看服务器的 TCP 连接情况来判断是否遭受 SYN Flood 攻击。

启用NAM的TCP Session信息监控。单击[Admin/Configure/Startup Options]菜单项，进入NAM配置界面。把Enable Session Handling (-z)配置为Yes，如图 3-59所示。

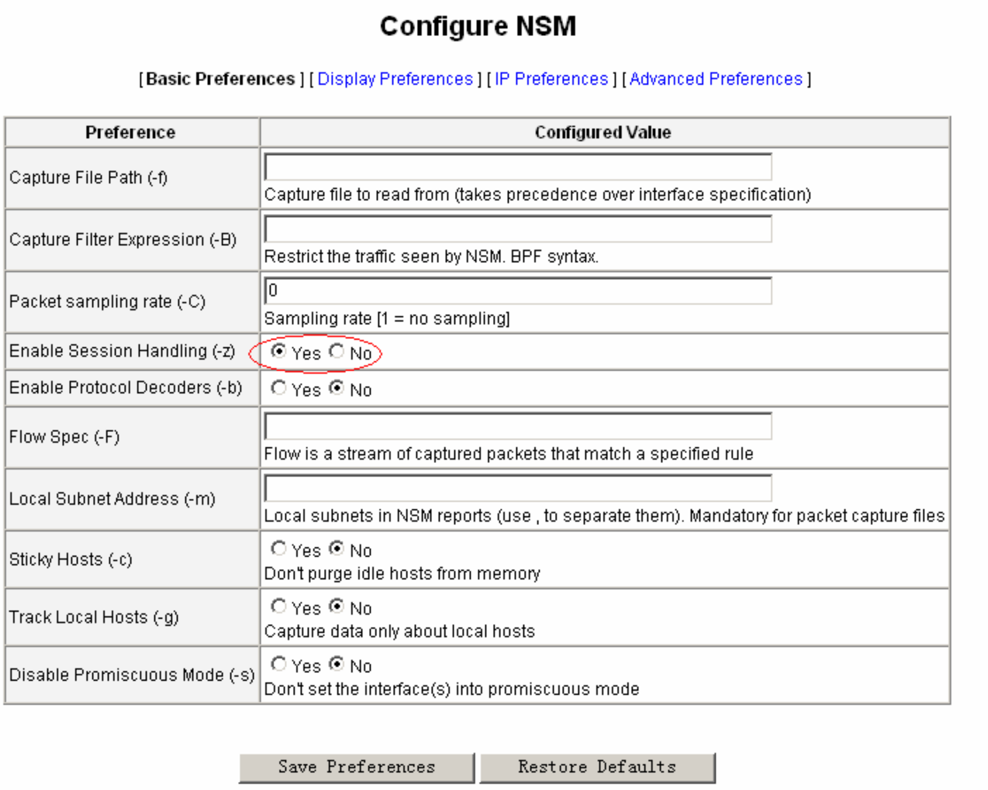


图3-59 NAM 配置页面

保存配置并重启 NAM。重启完毕后，NAM 使能了监控 TCP Session 的功能。

单击[Summary/Hosts]菜单项，点击待查看的服务器的IP，进入服务器的详细信息界面。直接查看Packet Statistics表，如图 3-60所示，表中显示了服务器的TCP 连接情况。如果发现收到了很多SYN报文，但没有收到对应的ACK报文，即可初步判断服务器收到了SYN Flood 攻击。

Packet Statistics

TCP Connections	Directed to		Rcvd From	
Attempted	2	11.0.0.12 11.0.0.13	4,496	11.0.0.11 11.0.0.15 11.0.0.19 11.0.0.12 11.0.0.13 11.0.0.17 11.0.0.16 11.0.0.18
Established	2 [100 %]	11.0.0.12 11.0.0.13	7 [0 %]	11.0.0.12 11.0.0.15 11.0.0.14 11.0.0.16 11.0.0.11
Terminated	0		4,485	11.0.0.11 11.0.0.15 11.0.0.19 11.0.0.12 11.0.0.13 11.0.0.17 11.0.0.16 11.0.0.18

TCP Flags	Pkts Sent		Pkts Rcvd	
SYN	2	11.0.0.12 11.0.0.13	4,496	11.0.0.11 11.0.0.15 11.0.0.19 11.0.0.12 11.0.0.13 11.0.0.17 11.0.0.16 11.0.0.18
RST|ACK	4,480	11.0.0.19 11.0.0.18 11.0.0.17 11.0.0.13 11.0.0.14 11.0.0.16 11.0.0.12 11.0.0.15	0	
RST	0		9	11.0.0.12 11.0.0.15 11.0.0.14 11.0.0.16 11.0.0.11 11.0.0.13

Anomaly	Pkts Sent to		Pkts Rcvd from	
Closed Empty TCP Conn.	0		4,485	• 11.0.0.11 • 11.0.0.15 • 11.0.0.19 • 11.0.0.12 • 11.0.0.13 • 11.0.0.17 • 11.0.0.16 • 11.0.0.18

图3-60 Packet Statistics 表

从上图可以看出服务器收到了 4496 个 TCP 的 SYN 报文，而只有 2 个是有效的，由此判定服务器正在受到 SYN Flood 攻击。

- 查看服务器的 ICMP 流量来判断是否遭受 ICMP Flood 攻击。

在同一个页面中，查看ICMP流量情况，如图 3-61所示。

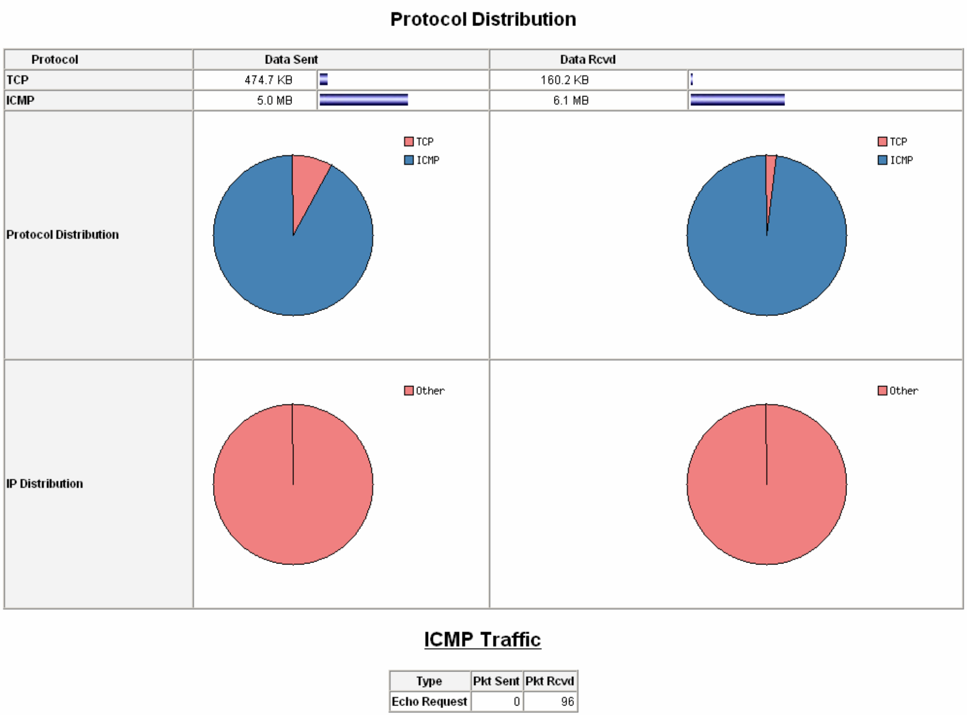


图3-61 ICMP 流量情况

发现 ICMP 流量很大，说明服务器收到非正常的 ICMP 流量。

单击[Plugins/ICMP Watch/View]菜单项，进入ICMP报文信息统计界面，如图 3-62所示。

ICMP Statistics

Host	Bytes		Sent/Recived by ICMP Type										
	Sent	Rcvd	Echo Request	Echo Reply	Time Exceeded	Unreach	Redirect	Router Advert.	Param. Problem	Network Mask	Source Quench	Timestamp	Info
192.168.0.11	2.4 MB	2.9 MB	0/46										
192.168.0.205	2.9 MB	2.4 MB	46/0										

图3-62 ICMP 报文信息统计界面

在此界面中，可以定位到发送 ICMP 报文的主机。

(2) 分析结果

从 NAM 的各种报表中发现，服务器的大量 TCP 连接都是无效的。而且服务器还同时收到了大量的 ICMP 报文。这些都消耗了服务器大量的资源，导致服务器无法提供正常的网络服务。

4. 建议网络管理员采取的措施

配置相应的路由器设置，来减少 DOS 攻击，可以参考下面配置方法：

- 禁止对服务器的非开放服务的访问。
- 限制同时打开的 SYN 最大连接数。
- 限制特定 IP 地址的访问。
- 启用路由器的防 DDoS 的属性。
- 严格限制对外开放的服务器对外访问的权限。

3.2.7 网络安全漏洞检测（二）病毒探测

1. 组网需求

在企业网中，经常因为某台 PC 中毒而导致病毒在网络中泛滥。更令人头疼的是，企业中的一些员工缺乏防病毒知识，而且防病毒意识淡薄。网络管理员如果能尽早发现病毒，就能及时采取措施，防止病毒在网络中的蔓延。同时定位到问题主机，及时进行杀毒和修复，消除安全隐患。

图 3-63为某企业的网络拓扑图，NAM集成于企业的出口路由器上。近来，企业内部有不少员工抱怨网络速度缓慢，不能正常使用网络服务。网络管理员将对这一情况进行排查和分析，其中使用了NAM来帮助定位问题。

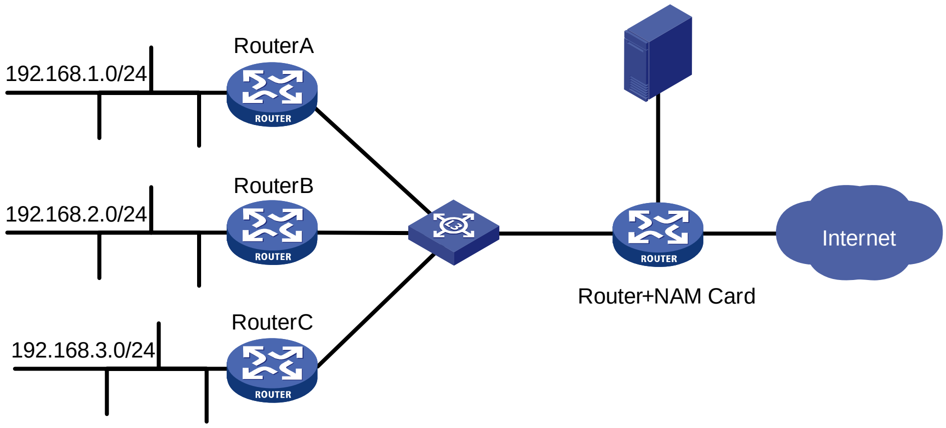


图3-63 病毒探测组网图

2. 环境分析

因为有较多员工反映网络速度缓慢，不能正常使用网络服务。因此初步判断网络中存在大量的无效报文，浪费了大量的带宽。在网络管理员的建议下，员工之间进行了主机互 ping 操作，发现 ping 时严重丢包。而且在没有网络连接的情况下，一些主机的网卡流量也比较大。根据这些信息，网络管理员判断网络中存在病毒。

如图 3-63所示，企业使用路由器连接Intranet和Internet。Intranet主要由三个网段组成：192.168.1.0/24、192.168.2.0/24、192.168.3.0/24。为了同时监控Intranet内部的流量，分别在RouterA，RouterB，RouterC上使用NetFlow采集流量，NetFlow目的端口为默认的 2055，目的IP为路由器的NAM的管理IP。

经过以上配置，网络管理员只需登录 NAM，即可查看 NAM 提供的流量统计图表，对网络中感染病毒的主机进行定位。另外，有些异常流量发生时并不体现为大流量，此时需要综合异常流量发生时的其它现象来判断，这些现象表现为：设备端口的包转发速率异常、网络时延较大、丢包严重、网络设备的 CPU 利用率频繁变化等。

说明：

关于NAM中NetFlow插件的典型应用，请参见3.2.1 网络流量统计（一）NetFlow流量分析。

---

3. 结果查看及分析

(1) 相关配置

配置NetFlow插件。具体请参见3.2.1 网络流量统计（一）NetFlow流量分析。

(2) 查看结果

- 查看当前活动的 TCP/UDP 的端口

单击[Summary/Traffic]菜单项，直接找到TCP/UDP Traffic Port Distribution表，如图 3-64所示。

TCP/UDP Traffic Port Distribution: Last Minute View

TCP/UDP Port		Total	Sent	Rcvd
10000	10000	10.8 MB	10.8 MB	0
ms-sql-m	1434	10.8 MB	0	10.8 MB

Notes:

- sum(total traffic per port) = 2*(total IP traffic) because the traffic per port is counted twice (sent and received)
- This report includes broadcast packets

图3-64 TCP/UDP Traffic Port Distribution 表

在表中发现一个可疑端口 1434，而把 1434 作为目的端口正是 2003 蠕虫王的典型特征。

- 查看使用特定目的端口的主机

为了进一步确定哪些主机在发送目的端口为 1434 的报文，点击相应的端口号链接，进入如图 3-65所示的界面。

Recent Users of Port 1434 (ms-sql-m)

Client	Server
• 192.168.1.19 • 192.168.1.29	• 192.168.1.41 • broadcast

图3-65 Active TCP/UDP Sessions 表

在表中可以看出是 192.168.1.19 和 192.168.1.29 在向 192.168.1.41 发送目的端口为 1434 的 UDP 报文。以此判断 192.168.1.19 和 192.168.1.29 已感染了 2003 蠕虫王病毒。

说明：

上述检测方式是实时检测，是以最近 1 分钟流量中的端口信息作为判断的依据。若要查看较长时间的监控结果，可以查看[IP/Local/Ports Used]界面下的端口信息（查看这些信息时，需要在[Admin/Configure/Startup Options]界面下把 Local Subnet Address (-m)参数设置为需要监控网段）。

---

(3) 分析结果

以上通过 NetFlow 插件，可以清晰的定位 Intranet 中感染病毒的机器以及感染的病毒（需要网络管理员事先了解病毒的特征）。

如果需要发现来自Internet对Intranet的蠕虫传播，需要检查来自Internet的TCP flag设置为RST/ACK的流记录。Intranet中的主机即使关闭了相应端口也会向来自Internet的TCP请求回应RST/ACK，如3.2.6 网络安全漏洞检测（一）DOS攻击检测中的图 3-60所示。这些回应了RST/ACK的主机就有可能被蠕虫病毒感染，网络管理员应该认真排查这些回应了RST/ACK的主机，及时发现病毒。

4. 建议网络管理员采取的措施

(1) 切断连接

在问题主机可控的情况下，切断问题主机的物理连接是最直接的办法，需要最先执行。

(2) 配置ACL过滤规则

在相关网络设备上配置 ACL（Access Control List）过滤规则，能够灵活实现针对源/目的 IP 地址、协议类型、端口号等各种形式的过滤，有效防止病毒扩散。同时也带来两个副作用：

- 消耗网络设备的系统资源
- 如果过滤条件设置不当，有可能过滤一些与病毒类似的正常报文，限制了一些正常的网络访问。

网络管理员可以谨慎的采用这一方法。

(3) 配置静态空路由过滤

在可以确定异常流量目的地址的情况下，可以相关网络设备上用静态路由把异常流量的目的地址指向空（Null）。这种过滤几乎不消耗网络设备的系统资源，但同时也完全阻断了对目的地址的正常访问。

网络管理员可以根据实际情况（如病毒严重程度，目的地址的使用频度等）谨慎使用这一方法。

通过以上方式可以防止病毒的扩散，之后需要网络管理员进行有效的杀毒。

3.2.8 网络优化和规划（一）网络冗余协议探测

1. 组网需求

在企业网中，IP 是最常用的网络通信协议。而企业员工经常会安装一些无用的网络协议，如 IPX、NetBIOS 等。这些协议经常广播报文，浪费了网络带宽。网络管理员可以定期普查网络协议的使用状况，发现并指导企业员工把这些无用的协议删除，优化网络环境。

图 3-66为某企业的网络拓扑图，NAM集成于企业的出口路由器上。网络管理员定期使用NAM对网络协议进行查看，如果发现冗余协议，并定位到具体的主机，即可指导企业员工进行删除。

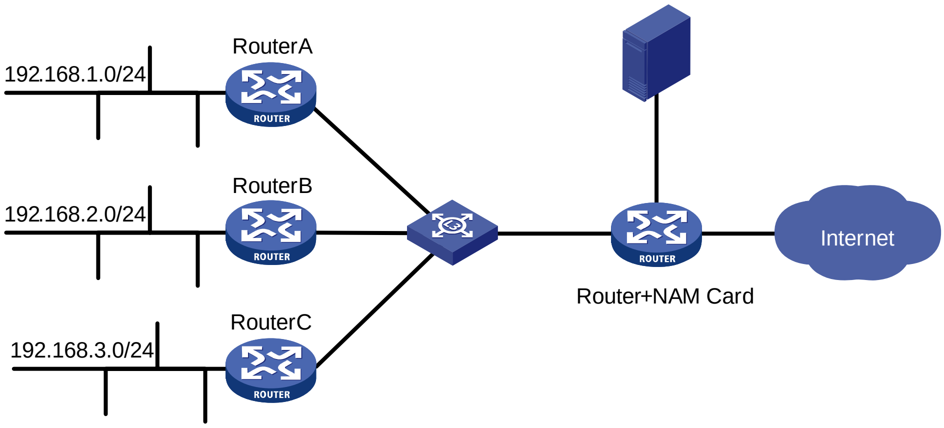


图3-66 网络冗余协议探测组网图

2. 环境分析

如图 3-63所示，企业使用路由器连接Intranet和Internet。Intranet主要由三个网段组成：192.168.1.0/24、192.168.2.0/24、192.168.3.0/24。为了监控Intranet内部的网络层协议，分别在RouterA，RouterB，RouterC上使用sFlow采集流量，sFlow目的端口为 6343，目的IP为路由器的NAM的管理IP。

经过以上配置，网络管理员只需登录 NAM，即可查看 NAM 提供的流量统计图表，对网络层协议进行查看。

📖 说明：

RouterA 等设备上 sFlow 的相关配置，请参见设备的配置手册。

---

3. 结果查看及分析

(1) 相关配置

NAM 提供 sFlow 插件作为 sFlow 分析工具，必须按照以下三个步骤进行正确的配置。

- 激活 sFlow 插件

单击[Plugins/sFlow/Active]菜单项，激活 sFlow 插件。

📖 说明：

若此菜单项显示为 Deactive，说明插件已经激活。

- 添加并配置 sFlow 虚拟接口

单击[Plugins/sFlow/Configure]菜单项，进入如图 3-67所示的界面。

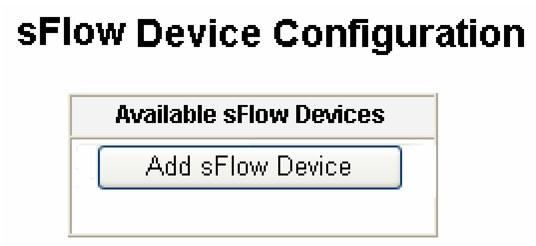


图3-67 Plugins/sFlow/Configure 界面

单击<Add sFlow Device>按钮，即可创建sFlow虚拟接口，并进入虚拟接口配置界面，如图 3-68所示。

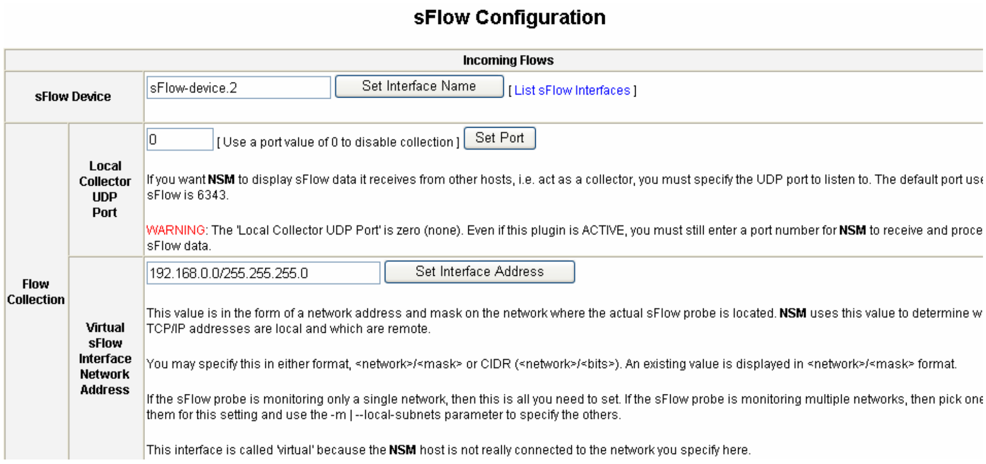


图3-68 sFlow 接口配置界面

需要对参数进行如下配置：

sFlow Device（interface name）：sFlow

Local Collector UDP Port：6343

Virtual sFlow Interface Network Address：192.168.0.0/16

其他参数均使用默认值。

- 切换网络接口

单击[Admin/Switch NIC]菜单项，进入如图 3-69所示的界面。把接口切换到sFlow接口。

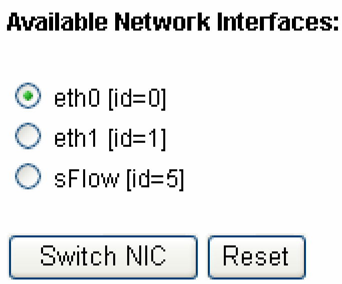
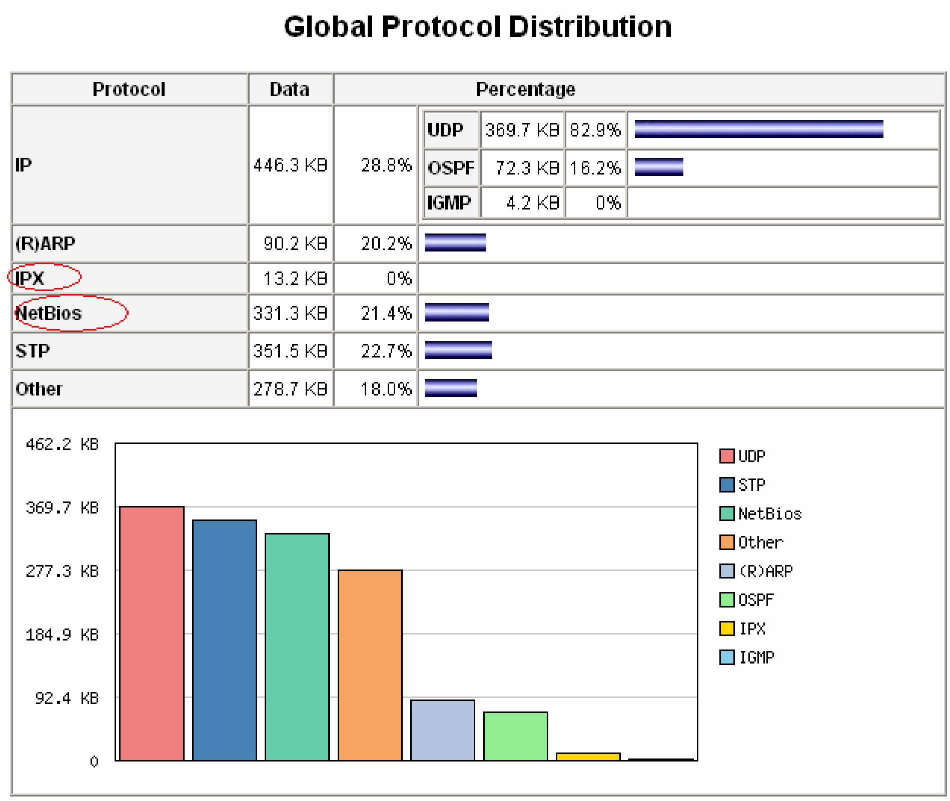


图3-69 切换接口界面

(2) 查看结果

- 查看全局流量，确定网络中包含协议的类型。

单击[Summary/Traffic]菜单项，直接找到Global Protocol Distribution表，如图 3-70 所示。



Global Protocol Distribution

Protocol	Data	Percentage			
IP	446.3 KB	28.8%	UDP	369.7 KB	82.9%
			OSPF	72.3 KB	16.2%
			IGMP	4.2 KB	0%
(R)ARP	90.2 KB	20.2%			
IPX	13.2 KB	0%			
NetBios	331.3 KB	21.4%			
STP	351.5 KB	22.7%			
Other	278.7 KB	18.0%			

图3-70 Global Protocol Distribution 表

在表中可以看出网络中存在 IPX、NetBIOS 流量。网络管理员需要定位到安装了这些协议的主机。

- 定位运行了 IPX 和 NetBIOS 的主机。

单击[All Protocols/traffic]菜单项，直接找到 Network Traffic 表，按照 IPX、NetBIOS 协议的流量对主机排序，找出使用了 IPX 或 NetBIOS 的全部主机，如所示。

Network Traffic [All Protocols]: All Hosts - Data Sent+Received

Hosts: [All] [Local Only] [Remote Only]

Host	Domain	Data		TCP	UDP	ICMP	ICMPv6	DLC	IPX	Decnet	(R)ARP	AppleTalk	NetBios	OSI	IPv6
192.168.0.169		731.8 KB	23.6 %	0	0	0	0	0	0	0	504	0	508.8 KB	0	0
netbios:00:00:01		508.8 KB	16.4 %	0	0	0	0	0	0	0	0	0	508.8 KB	0	0
bridge sp. tree/osi route:00:00:00		504.8 KB	16.3 %	0	0	0	0	0	0	0	0	0	0	0	0
192.168.1.57		309.2 KB	10.0 %	0	309.2 KB	0	0	0	0	0	0	0	0	0	0

Network Traffic [All Protocols]: All Hosts - Data Sent+Received

Hosts: [All] [Local Only] [Remote Only]

Host	Domain	Data		TCP	UDP	ICMP	ICMPv6	DLC	IPX	Decnet	(R)ARP	AppleTalk	NetBios	OSI
192.168.0.198		18.9 KB	0.5 %	0	0	0	0	0	18.4 KB	0	500	0	0	0
192.168.0.204		1.1 KB	0.0 %	0	0	0	0	0	918	0	250	0	0	0
d-link corporation:f5:98:05		518	0.0 %	0	0	0	0	0	518	0	0	0	0	0
EC:57:00:00:42:49		130	0.0 %	0	0	0	0	0	0	0	0	0	0	0

图3-71 Network Traffic 表

根据主机的 IP 地址，即可定位到具体的主机。

4. 解决问题

网络管理员找到对应的主机，确认此主机不需要使用 IPX 或 NetBIOS，把相应的协议删除即可。

5. 注意事项

Global Protocol Distribution表（图 3-70）中统计的NetBIOS，包含了TCP/IP的NetBIOS（NetBT）流量和NetBEUI流量。早期的Windows及其他操作系统需要使用NetBEUI协议来进行通信，新版本的Windows都使用TCP/IP的NetBIOS（NetBT）来进行通信。

使用 NetBEUI 协议的操作系统包括：Microsoft Windows NT Server 3.5 或者更新版本、Microsoft Windows NT、Workstation 3.5 或更新版本、Microsoft LAN Manager、Microsoft Windows for Workgroups、Microsoft Windows 3.1、Microsoft Windows 95、Microsoft Windows 98、Microsoft WindowsNT3.1、LAN Manager for UNIX，以及 IBM PCLAN 和 LAN Server。

在[All Protocols/Traffic]菜单项对应的界面中，查看 NetBIOS 列，此列显示了非 NetBT 类型的 NetBIOS 报文，即 NetBEUI 报文。

如果发现网络中有 NetBEUI 协议，请在删除时确认主机的操作系统，避免因为误删出而导致主机无法通信。

第4章 常见问题解答

1. 在局域网中配置了很多 VLAN，而在 NAM 软件中只能监控到 1 个 VLAN 的流量。这是为什么？

如果需要监控局域网中的所有 VLAN，被监控接口必须配置为 trunk 类型，同时把需要监控的 VLAN 配置为允许通过。这样即可监控相应 VLAN 的流量。

2. 在[IP/Local]菜单下没有 Active TCP/UDP Sessions 菜单项，这是为什么？

这是因为[Admin/Configure/Startup Options]对应的页面中，Basic Preferences 下的 Enable Session Handling (-z)参数没有配置为 Yes。只需该参数配置为 Yes，即可看到[IP/Local/Active TCP/UDP Sessions]菜单项。

3. 为什么广播报文总是被统计 2 次？

通常情况下，被监控端口都配置了镜像，镜像流量被统计 1 次。同时，广播报文会在所在的 VLAN 中泛洪，监控端口也会接收到此泛洪，于是再被统计 1 次。因此一共会被统计 2 次。

4. Host 列有时显示为节点的 FQDN（Fully Qualified Domain Name，正式域名）名称，有时为节点的 IP 地址，有时为 MAC 地址。这是为什么？

若 NAM 启动时的配置参数 No DNS(-n)为 no（具体请参见附录 A.7.2.1），则 NAM 会把探测到的 IP 地址试图解析成相应的 FQDN 名称。如果解析成功，则在 Host 列显示 FQDN 名称，否则显示 IP 地址。若 NAM 启动时的配置参数 No DNS(-n)为 yes，则 NAM 不对探测到的 IP 地址进行解析，直接显示为 IP 地址。若 NAM 探测到的报文不是基于 IP 的（如：STP、IPX 等），则显示为 MAC 地址。

5. 为什么 Domain 有时能取到值，有时取值错误？

只有 IP 地址解析成相应的 FQDN 名后，才能显示正确的 Domain。Domain 列通常以图标的方式显示。如果 IP 地址不属于私有 IP 地址范围（10.0.0.0/8、176.16.0.0/12 或 192.168.0.0/16），则 NAM 会查找 p2c.opt.table.gz 文件，从中找出 IP 地址与国家的对应关系，然后以相应的国旗表示。如果 p2c.opt.table.gz 文件中包含的不是最新的对应关系，则 IP 地址与国家的对应关系可能出错。

可以到相应网站下载最新的信息，也可以手工编辑配置文件（甚至添加新的国家图标）来更新 IP 与国家的对应关系。点击 NAM 对应页面中的 NOTE 下面的 here 链接，可查看详细步骤。

6. 为什么重启 NAM 软件后所有的数据都丢失了？

NAM 把正在使用的数据都保存在内存中，所以重启 NAM 软件后这些数据会丢失。历史数据保存在 RRD 数据库中，激活 RRD 插件后，即可查看历史数据。

7. NAM 正在运行，为什么看不到任何流量？

在[Admin/Switch NIC]中查看监控端口是否正确。如果端口配置正确却没有流量，请查看路由器上端口 GigabitEthernet 1/0 流量情况，只有 GigabitEthernet 1/0 的流量会被统计。

8. 在[Admin/Configure/Startup Options]的 Advanced Preferences 中配置了 Don't Merge Interfaces (-M)参数（主要用于合并端口），为什么这一配置不生效。？

在 NAM 软件中，如果启用了 NetFlow 或 sFlow 插件，则 Don't Merge Interfaces (-M)不生效。

9. 为什么设定 Capture File Path 参数以后，NetFlow 和 sFlow 虚拟接口还有效？

因为两者并不冲突。

Capture File Path 参数的含义是从文件中读取报文数据，NetFlow、sFlow 虚拟接口则打开了相应的 UDP 端口监听数据。两者的数据来源不同，不会冲突。NAM 都会进行统计。

10. Preferences 的配置和 Startup Options 配置有什么不同？

Preference 和 Startup Options 中的参数表现形式不同，而且 Preferences 中的参数更加齐全。Preferences 和 Startup Options 中的参数配置的效果相同。

11. 使用[Admin/Configure/Reset Stats]清空数据，再查看页面时还存在数据，这是为什么？

[Admin/Configure/Reset Stats]清空了内存中的数据。进行了清空操作之后，页面还会有显示两种数据：

- 清空操作之后，NAM 实时监控的流量。
- 某些存放在磁盘中的数据，如[Summary/Network Load]中显示的数据。

12. NAM 中的 local 和 remote 是怎么定义的？

[Admin/Configure/Startup Options]中的 Local Subnet Address 参数用于配置 local 的范围。

举例说明如下：

配置了 Local 的范围为 1.2.3.0/24

源为 1.2.3.0/24、目的为 1.2.3.0/24 的数据属于 local->local。

原为 1.2.3.0/24、目的为 131.114.21.9 的数据属于 local->remote。

remote->local 和 remote->remote 类似。

13. 为什么在 NAM 中不能得到 RRD 的输出？

(1) 确认 RRD 插件是否使能

(2) 缺省情况下，没有为每个主机保存一个 RRD 文件。如果需要输出某个主机的流量，需要在[Admin/Configure/Startup Options]中通过 Local Subnet Address 参数配置该主机所在的子网和掩码。

14. 日志 What do these log messages mean 是什么意思？

出现这个日志的原因是 NAM 发现同一个主机的报文（同一个 IP 和 MAC）属于不通的 VLAN。NAM 软件发现一个报文就统计一个报文，有可能出现重复统计。因此这不是问题。

15. 什么是 What are High/Medium/Low risk flags？

NAM 软件具有一定的告警功能。当主机的某些配置或者网络行为符合 NAM 中的某些设定时，就会显示 risk flag。不同颜色的 risk flag 用于提示主机不同的配置或网络行为。具体情况可以参见 NAM 软件页面中对 risk flag 的说明。

16. 为什么有的主机名以不同的颜色显示？

这是为了表达主机的一些特殊信息。例如：ACTIVE TCP SESSIONS 中用五种不同的颜色表示主机距第一次被 NAM 捕获到报文的时间。

17. 为什么不能通过 WEB 界面访问 NAM？

(1) 请确认NAM是否已经启动，具体操作请参见2.3.6 启动和关闭NAM软件。

(2) 请确认使用的访问方式是否正确，即需要正确使用 http 或 https 来访问 NAM。

18. 如何查看[IP/Summary/Host Clusters]中 Cluster 流量？

Cluster 是管理员根据自身需要配置的网段，在[Admin/Configure/Preferences]中设置。格式为：cluster.myCluster = 网段范围，其中 myCluster 为管理员自定义的网段名称，网段范围格式如下所示：169.254.0.0/16，192.168.0.0/16，可以设置一个或者多个网段。

19. 网络管理员发现，有时候网络中没有 eDonkey 等流量，在 NAM 的统计图表中却显示这些流量非 0。这是为什么？

因为 NAM 对于这些协议的统计是基于端口号的，如果网络中的某些报文使用的端口号恰好与这些协议的相同，那么就会出现上述情况。

20. 什么是 BPF 表达式？

BPF 是一种过滤机制，用于筛选需要关注的报文。BPF 表达式是一种基本的格式，表示了筛选报文的条件。

BPF 表达式一般由三种类型的原语组成：

Type：host、net、port

Dir：src、dst、src or dst、src and dst

Proto：ether、fddi、ip、arp、rarp、decnet、lat、sca、moprc、mopdl、tcp、udp

各原语用 and、or、not 连接。

如：src host 192.168.1.1 and dst host 192.168.1.2 就表示筛选源为 192.168.1.1，目的为 192.168.1.2 的报文。

表4-1 常见原语表

常见的基本原语	常见的基本原语	常见的基本原语
dst host *host*	src net *net*	greater *length*
src host *host*	net *net*	ip proto *protocol*
host *host*	net *net* mask *mask*	ether broadcast
ether dst *ehost*	net *net/len*	ip broadcast
ether src *ehost*	dst port *port*	ether multicast
ether host *ehost*	src port *port*	ip multicast
gateway *host*	port *port*	ether proto *protocol*
dst net *net*	less *length*	

说明：

上表中正体字表示原语中的关键字；斜体字表示原语中的参数，需要原语使用者自定义。

21. 在历史数据（Historical Data）统计图中，报文的各种统计值后面的字母分别表示什么含义?

在报文的分类统计图中，统计值均省略了计数单位 Bytes，如 1.3k 表示 1.3k Bytes，1.3M 表示 1.3M Bytes。

统计值后面的字母（区分大小写）表示该统计值的数量级。每个字母的具体含义请参见表 4-2。

表4-2 字母含义表

字符	含义
a	10e-18(Ato) Bytes
f	10e-15(Femto) Bytes
p	10e-12(Pico) Bytes
n	10e-9(Nano) Bytes
u	10e-6(Micro) Bytes
m	10e-3(Milli) Bytes
无	Bytes
k	10e3(Kilo) Bytes
M	10e6(Mega) Bytes
G	10e9(Giga) Bytes
T	10e12(Terra) Bytes
P	10e15(Peta) Bytes
E	10e18(Exa) Bytes

22. 在历史数据（Historical Data）统计图中，为什么存在以下两种情况？

- 小流量报文统计值对应的纵坐标比大流量报文统计值对应纵坐标值还大。
- 某些类型报文的统计值和其在图中对应的纵坐标不相符。

为了清晰显示代表各种类型报文的颜色，第二种报文的图形会以第一种报文的数值对应的纵坐标作为 y 坐标轴的原点进行绘制，以此类推。因此，当查看图中纵坐标不是从 0 开始的色块所代表的报文数值时，正确值为该色块对应的纵坐标最大值和最小值之差。

23. 在历史数据（Historical Data）统计图中，为什么有时图形会显示在坐标轴下方？

这是因为此时图中的 x 坐标轴对应的纵坐标数值不为 0。

24. 修改了 Linux 的系统时间后，NAM 中的许多统计值都出现了错误，如平均报文速率出现了负数值。这是为什么？

NAM 收集的流量信息都是时间敏感数据，在计算各种统计值时会使用当前系统时间。如果修改了 Linux 的系统时间，就会导致各种统计值计算错误，甚至出现负数值的情况。因此请不要轻易修改 Linux 的系统时间。如果确实需要修改，请在修改后重新启动 NAM 软件。

目 录

附录 A NAM 软件功能详解

A.1 Summary

A.1.1 Traffic

此界面显示了网卡探测到的所有流量的信息，如被监控端口上的报文大小、流量的 TTL 值分布、各种协议的分布情况等。还能以日、月、年的方式显示历史流量的分布，方便网络管理员判断网络拥塞发生的时间和起因（何种协议造成了拥塞）。

1. Global Traffic Statistics

显示了本地配置的一些基本信息。

表A-1 Global Traffic Statistics

表项	含义
Network Interface	包含了所有监控接口及其属性，包括：名称、设备、类型、接口速率、采样速率、MTU、头部长度、IPv4 地址、IPv6 地址
Local Domain Name	通常为国家名称，可以通过[Admin/Configure/Startup Options]菜单项对应页面中的 IP Preferences 下的 Local Domain Name 参数进行配置
Sampling Since	NAM 启动的时间
Active End Nodes	当前网络中探测到的主机节点的数量

说明：

若需要统计 IPv6 流量，需要在 NAM 服务器上安装 IPv6 协议并配置相应的 IPv6 地址。

2. Traffic Report

详细分析了被监控端口，包括对报文的分析、对流的分析以及流量负载情况。

表A-2 Traffic Report for 'eth0'

表项		含义
Packets	Dropped (libpcap)	因网络太忙导致被 libpcap 丢弃的报文数量
	Dropped (NAM)	因服务器太忙导致被 NAM 丢弃的报文数量
	Total Received (NAM)	NAM 接收的报文数量
	Total Packets Processed	NAM 已经处理的报文数量
	Unicast	接收的单播报文数量
	Broadcast	接收的广播报文数量
	Multicast	接收的多播报文数量
	Shortest	收到报文的最小长度值
	Average Size	收到报文的平均长度值
	Longest	收到报文的最大长度值
	各种长度范围	各种长度报文数量的统计
	Packets too long [> 1518]	超长报文的数量
	Bad Packets (Checksum)	校验和错误的报文数量
Traffic	Total	收到的流量总和
	IP Traffic	收到的 IP 流量的总和
	Fragmented IP Traffic	收到的 IP 分片流量的总和
	Non IP Traffic	收到的非 IP 流量的总和
	Average TTL	收到的数据流的 TTL 平均值
	各种 TTL 大小	各种 TTL 大小的统计
Network Load	Actual	当前的网络负载情况
	Last Minute	最近 1 分钟的网络负载情况
	Last 5 Minutes	最近 5 分钟的网络负载情况
	Peak	网络负载峰值情况
	Average	网络负载平均值
Historical Data		此链接可以以图形的方式查看历史数据的分布情况。分别查看最近 1 小时、6 小时、12 小时、1 天、1 星期、1 个月、1 年的流量

说明：

- 所有历史数据都存储在 RRD 数据库中，所以执行 NAM 中的 Reset Stats 命令并不清空历史数据。要想调整历史数据的显示，需要配置 RRD 插件。
- 如果达到了最大的 TCP 连接数，则 libpcap 将丢弃之后收到的报文。最大的 TCP 连接数可以通过[Admin/configure/Startup Options]菜单项所对应的页面中的 advanced preferences 参数查看。

3. Global Protocol Distribution

显示了被监控端口上的协议情况，给出了各种协议类型及对应的大小、百分比，并以柱状图的方式显示了各种协议的分布情况。

表A-3 Global Protocol Distribution

表项	含义
Protocol	探测到的协议类型
Data	对应协议的数据大小
Percentage	各个协议占总流量的百分比

4. Global TCP/UDP Protocol Distribution

显示了所有探测到的 TCP/UDP 协议类型，以图表的形式分别按照协议流量大小、流数量、累积的百分比和历史百分比进行显示，其中历史百分比用柱状图显示。

表A-4 Global TCP/UDP Protocol Distribution

表项	含义
TCP/UDP Protocol	协议类型
Data	对应协议的流量大小
Flows	对应协议的流数量。若协议类型为 TCP，则 1 个 TCP 连接对应 1 条流。若协议类型为 UDP，则 1 个 UDP 报文对应 1 条流

说明：

若 TCP 的客户端与服务器端的连接类型为双向的，TCP 类型的流数量统计算作 1。

5. TCP/UDP Traffic Port Distribution Last Minute View

显示了最近 1 分钟内探测到的 TCP/UDP 端口的数据流的统计情况，包括端口号、总的报文数、发送报文数、接收报文数。

表A-5 TCP/UDP Traffic Port Distribution Last Minute View

表项	含义
TCP/UDP Port	探测到的报文的 TCP/UDP 端口号
Total	对应端口的所有报文数量
Sent	对应端口的发送报文数量
Rcvd	对应端口的接收报文数量

说明：

该页面的统计信息包含广播报文数量。

A.1.2 Hosts

显示了主机信息，分别以字节、报文为单位显示，同时又可以基于 VLAN 来查看不同的主机信息。更强大的功能是，它每一列都支持排序，方便用户很快的查询到所需要的信息。

表A-6 Hosts

表项	含义
Host	列出了探测到的主机，会以 IP、MAC 、主机名方式显示，同时又会链接到相应的主机信息
Domain	主机对应的域名
IP Address	主机的 IP 地址
MAC Address	主机的 MAC 地址
Other Name	主机的别名
BandWidth	主机的发送和接收带宽，分别以绿色和蓝色表示，绿色代表发送，蓝色代表接收。
Nw Board Vendor	主机的网卡对应的厂商名称
Hops Distance	主机与 NAM 之间的跳计数
Host Contacts	主机与 NAM 的联系次数
Age/Inactivity	主机与 NAM 的联系时间和非活动时间
AS	主机所属的 AS 号

📖 **说明：**

当将鼠标停留在Bandwidth列下面的图形时，会显示此主机占用的实际带宽值。因为本地流量可能会被统计 2 次（发送和接收），所以所有流量百分比的和有可能不是100％。

A.1.3 Network Load

1. Network Load Statistics

显示了被监控接口的网络负载情况。所有的数据是从 RRD 数据库中获取的，分别以 4 个时段来显示。

表A-7 Network Load Statistics

表项	含义
Last 10 Minutes Throughput	近 10 分钟的网络负载情况，分别显示最小值、最大值、平均值、当前值。点击视图会查看最近 10 分钟网络负载的具体信息，具体描述请参见A.1.3 2. Network Load Statistics Matrix
Last Hour Throughput	最近 1 小时的网络负载情况，分别显示最小值、最大值、平均值、当前值
Current Day Throughput	最近 1 天的网络负载情况，分别显示最小值、最大值、平均值、当前值
Last Month Throughput	最近 1 月的网络负载情况，分别显示最小值、最大值、平均值、当前值

📖 **说明：**

若向修改监控的频率，点击本页的右下方链接会进入RRD配置界面，进行相应的修改，详细配置信息请参见A.6.5 Round-Robin DataBase。

2. Network Load Statistics Matrix

显示了采样间隔为 1 分钟的流量情况，以矩阵的方式显示了平均网络流量，以及发送和接收流量排名前 3 位的主机的名称。

表A-8 Network Load Statistics Matrix

表项	含义
Sampling Period	采样时间，以 1 分钟为单位
Average Thpt	平均流量值
Top Hosts Sent Thpt	流量发送排名前 3 位的主机的名称及对应的流量值

表项	含义
Top Hosts Rcvd Thpt	流量接收排名前 3 位的主机的名称及对应的流量值

A.1.4 VLAN Info

显示了基于 VLAN 方式统计的流量值。

表A-9 VLAN Info

表项	含义
VLAN	列出了探测到的 VLAN
Hosts	列出了 VLAN 中的主机列表
Data Sent	对应 VLAN 发送的报文量
Data Rcvd	对应 VLAN 接收的报文量

说明：

只有配置了相应的 VLAN 后此菜单才可见。

A.1.5 Network Flows

主要显示了 Host Last Seen 插件和用户自定义的流规则的流量情况。

表A-10 Network Flows 功能简介

表项	含义
Flow Name	列出了插件 Host Last Seen 或者用户自定义流规则的名称
Packets	报文数量
Traffic	流量大小

说明：

- 只有插件 Host Last Seen 启用后，此界面才有该插件的统计信息。
- 如果是用户自定义的流规则，例如 ICMP='icmp'，其中 ICMP 是流规则的名称，单引号内的 icmp 为流规则，流规则必须是一个合法的 BPF 表达式。

A.2 All Protocols

A.2.1 Traffic

显示了包含了所有协议的网络流量情况，包括所有主机的发送和接收报文情况。可以分别以本地和远程、发送和接收的方式显示。还可以以不同的 VLAN 划分来显示网络主机信息。且可以对列排序，快速找到流量分布情况。下面介绍界面的详细内容。

表A-11 Traffic

表项	含义
Host	此列显示了侦听到的主机的名称，以 IP、MAC、或主机名的方式显示
Domain	域名，一般为以国旗方式显示的国家
Data	数据值，分别以流量和百分比的方式显示
TCP	TCP 类型的报文的流量
UDP	UDP 类型的报文的流量
ICMP	ICMP 类型的报文的流量
ICMPv6	ICMPv6 类型的报文的流量
DLC	DLC 类型的报文的流量
IPX	IPX 类型的报文的流量
Decnet	Decnet 类型的报文的流量
(R)ARP	(R)ARP 类型的报文的流量
AppleTalk	AppleTalk 类型的报文的流量
NetBIOS	NetBIOS 类型的报文的流量
OSI	OSI 类型的报文的流量
IPv6	IPv6 类型的报文的流量
STP	STP 类型的报文的流量
IPSEC	IPSEC 类型的报文的流量
OSPF	OSPF 类型的报文的流量
IGMP	IGMP 类型的报文的流量
Other	Other 类型的报文的流量

📖 **说明：**

这里的统计不包含广播报文，所以与 Global Protocol Distribution 的显示略有不同。

A.2.2 Throughput

显示了所有协议的网络负载情况，包括所有主机的发送和接收报文情况。可以以本地和远程的方式显示，也可以以发送和接收的方式显示。且可以对列排序。下面以列表的方式介绍界面的详细内容。

表A-12 Throughput

表项	含义
Host	此列显示了侦听到的主机的名称，以 IP、MAC、或主机名的方式显示
Domain	域名，一般为以国旗方式显示的国家
Data	此列分别以 Current、Avg、Peak 方式显示了每个主机网络负载情况。单位是 bps
Packets	此列分别以 Current、Avg、Peak 方式显示了每个主机网络负载情况。单位是 Pkts/sec

📖 **说明：**

其中 Peak 显示的值为任何 60 秒间隔中的最大值。Avg 为 60 秒计算 1 次。所有这些值是 NAM 启动以来开始计算的。且每次 NAM 服务重启，这些值会重新计算。

A.2.3 Activity

显示了所有协议的网络活动情况，以 4 种颜色方式显示，包括所有主机的发送和接收报文情况。可以以本地和远程的方式显示，也可以以发送和接收的方式显示。且可以对列排序。下面以列表的方式介绍界面的详细内容。

表A-13 Activity

表项	含义
Host	此列显示了侦听到的主机的名称，以 IP、MAC、或主机名的方式显示
Domain	域名，一般为国家的名称。以国旗方式显示
Time	分为 24 列，每列对应 1 小时，显示了这 1 小时中的流量占最近 24 小时流量总和的百分比。以相应的颜色显示

A.3 IP

显示了 NAM 探测到的所有 IP 协议的流量信息，进一步细分为各种应用层协议，例如 FTP，HTTP 等等。可以按照主机信息为索引来显示各个主机使用的各个应用层协议的情况，用户也可以根据自己的需要配置子网来查看某个网段的主机的流量信息。Traffic Directions 可以查询所有主机之间的数据流向情况，Local 功能提供本地主机的端口使用情况、主机详细信息、TCP/UDP 会话信息、各个主机之间的详细数据流向、本地网络拓扑图等。

A.3.1 Summary

1. Traffic

显示了网络中所有主机使用的应用层协议流量信息。所有协议按照如下方式分类显示。

表A-14 所有主机流量显示方式分类图

表项		含义
按照 Hosts 区分	All	显示所有主机的信息
	Local Only	只显示本地主机的信息
	Remote Only	只显示远程主机的信息
按照 VLAN 区分	ALL	显示所有 VLAN 的信息
	VLAN 号	按照 VLAN 号区分
按照 Data 区分	All	显示所有有发送数据的或者接收数据的主机
	Sent Only	只显示有发送数据的主机
	Received Only	只显示有接收数据的主机

说明：

只有报文中携带了 VLAN 信息，才会有按照 VLAN 区分的显示

以主机为单位显示主机接收到和发送各种协议情况。

表A-15 Local Hosts - Data Sent+Received

表项	含义
Host	主机信息，一般为主机的 IP 地址（也可以是 DNS 名称或者 NetBios 等），以蓝色超链接形式，可以通过[summary/host]菜单项对应页面查看该主机信息，点击弹出新的页面显示此主机的具体流量等信息

表项	含义
Domain	域名，一般为国家的名称。以国旗方式显示
Data	对应主机流量的值
FTP	对应主机 FTP 类型的报文流量的值，包括 ftp 与 ftp-data
HTTP	对应主机 HTTP 流量的值
DNS	对应主机 DNS 流量的值
Telnet	对应主机 Telnet 流量的值
NBios-IP	对应主机 NBios-IP 流量的值，包括 netbios-ns、netbios-dgm、netbios-ssn
Mail	对应主机 Mail 流量的值，包括 pop-2 pop-3 pop3 kpop smtp imap imap2
DHCP-BOOTP	对应主机 DHCP-BOOTP 流量的值。
SNMP	对应主机 SNMP 流量的值
NNTP	对应主机 NNTP 流量的值
NFS/AFS	对应主机 NFS/AFS 流量的值
VoIP	对应主机 VoIP 流量的值
X11	对应主机 X11 流量的值
SSH	对应主机 SSH 流量的值
Gnutella	对应主机 Gnutella 流量的值
Kazaa	对应主机 Kazaa 流量的值
WinMX	对应主机 WinMX 流量的值
DC++	对应主机 DC++流量的值
eDonkey	对应主机 eDonkey 流量的值
BitTorrent	对应主机 BitTorrent 流量的值
Messenger	对应主机 Messenger 流量的值
Other IP	对应主机非以上各类协议流量的值

说明：

- 这里的统计不包含广播报文，所以与“Global Protocol Distribution”的显示不同。
- 所有的流量大小单位规则如下，如果不带单位，则表示是字节数；果流量较大，会按照流量大小以 KB、 MB 或者 GB 为单位显示。

2. Multicast

显示了网络的多播流量情况，包括所有主机的发送和接收报文情况。

表A-16 Multicast Statistics

表项	含义
Host	主机信息，一般为主机的 IP 地址（也可以是 DNS 名称或者 NetBios 等），以蓝色超链接形式，可以通过[summary/host]菜单项对应的页面查看该主机信息，点击弹出新的页面显示此主机的具体流量统计等信息
Domain	域名，一般为国家的名称。以国旗方式显示
Pkts Sent	发送的多播报文的数量，单位为个
Data Sent	发送的多播流量的值
Pkts Rcvd	接收的多播报文数量，单位为个
Data Rcvd	接收的多播流量的值

说明：

所有的流量大小单位规则如下，如果不带单位，则表示是字节数，如果流量较大，会按照流量大小以 KB、MB 或者 GB 为单位显示。如果没有多播报文，则显示 No Data To Display (yet)。

3. Internet Domain

本界面以 Domain 为单位显示了在该 Domain 中所有主机的一些统计信息，各参数含义如下所示。

表A-17 Statistics for all Domains

<table>
<tr><th colspan="3">表项</th><th>含义</th></tr>
<tr><td colspan="3">Name</td><td>Domain 的名称</td></tr>
<tr><td colspan="3">Domain</td><td>主机所在域域名，一般为国家的名称。以国旗方式显示</td></tr>
<tr><td rowspan="6">TCP/IP</td><td rowspan="2">Total</td><td>Sent</td><td>该 Domain 内所有主机发送的 TCP/IP 流量的值</td></tr>
<tr><td>Rcvd</td><td>该 Domain 内所有主机接收的 TCP/IP 流量的值</td></tr>
<tr><td rowspan="2">TCP</td><td>Sent</td><td>该 Domain 所有主机发送的 TCP 流量的值</td></tr>
<tr><td>Rcvd</td><td>该 Domain 所有主机接收的 TCP 流量的值</td></tr>
<tr><td rowspan="2">UDP</td><td>Sent</td><td>该 Domain 所有主机发送的 UDP 流量的值</td></tr>
<tr><td>Rcvd</td><td>该 Domain 所有主机接收的 UDP 流量的值</td></tr>
</table>

表项			含义
ICMP	IPv4	Sent	该 Domain 所有主机发送的 ICMP 报文中 IPv4 流量的值
		Rcvd	该 Domain 所有主机接收的 ICMP 报文中 IPv4 流量的值
	IPv6	Sent	该 Domain 所有主机发送的 ICMP 报文中 IPv6 流量的值
		Rcvd	该 Domain 所有主机接收的 ICMP 报文中 IPv6 流量的值

说明：

- 所有的流量大单位规则如下，如果不带单位，则表示是字节数，如果流量较大，会按照流量大小以 KB、 MB 或者 GB 为单位显示。
- 如果所有主机都没有 Domain 信息，那么此菜单将显示 No Data To Display (yet)。

4. Host Cluster

按照用户配置的网段及掩码显示该网段主机的流量信息。

表A-18 Statistics for all clusters

表项			含义
Name			该网段的名称，单击此网段名称可列出此网段所有主机发送和接收报文的情况
Domain			网段所在域域名，一般为国家的名称。以国旗方式显示
TCP/IP	Total	Sent	该网段内所有主机发送的 TCP/IP 流量的值
		Rcvd	该网段内所有主机接收的 TCP/IP 流量的值
	TCP	Sent	该网段所有主机发送的 TCP 流量的值
		Rcvd	该网段所有主机接收的 TCP 流量的值
	UDP	Sent	该网段所有主机发送的 UDP 流量的值
		Rcvd	该网段所有主机接收的 UDP 流量的值
ICMP	IPv4	Sent	该网段所有主机发送的 ICMP 报文中 IPv4 流量的值
		Rcvd	该网段所有主机接收的 ICMP 报文中 IPv4 流量的值
	IPv6	Sent	该网段所有主机发送的 ICMP 报文中 IPv6 流量的值
		Rcvd	该网段所有主机接收的 ICMP 报文中 IPv6 流量的值

📖 **说明：**

- 所有的流量大小单位规则如下，如果不带单位，则表示是字节数，如果流量较大，会按照流量大小以 KB、MB 或者 GB 为单位显示。
- 关于 Cluster 的设置，请参见正文 第四章 常见问题解答 的问题 18。

5. Distribution

显示了本地和远程流量的分布情况，首先是一个饼状图显示本地、远程->本地、本地->远程、远程 4 种流量的所占百分比情况，接下来以表格的方式分别显示了这四种流量的详细信息。

Local Traffic：本地到本地的所有主机流量情况。

Remote to Local Traffic：远程到本地的所有主机流量情况。

Remote Traffic：远程到远程的所有主机流量情况。

Local to Remote Traffic：本地到远程的所有主机流量情况。

四种流量表中的参数一致，请参见表A-19和表A-20。

表A-19 Traffic 参数（1）

表项		含义
IP Protocol		协议类型，即 TCP 和 UDP
Data		TCP 和 UDP 协议的流量总和
Percentage	TCP	TCP 协议流量所占百分比
	UDP	UDP 协议流量所占百分比

表A-20 Traffic 参数（2）

表项	含义
TCP/UDP Protocol	列出了哪种协议类型，例如 FTP 等，协议类型域[IP/Summary/Traffic]中 Network Traffic [TCP/IP]: All Hosts - Data Sent+Received 图所示协议的类型对应，有流量则显示，没有则不显示
Data	对应 TCP/UDP Protocol 下具体协议的流量总和
Percentage	对应 TCP/UDP Protocol 下具体协议占的百分比

A.3.2 Traffic Directions

1. Local To Local

显示了本网段主机的流量情况，参数意义如下。

表A-21 Local IP Traffic

表项	含义
Host	本地主机信息，如果与本地主机没有通信，则不显示。一般为主机的 IP 地址（也可以是 DNS 名称或者 NetBios 等），以蓝色超链接形式，可以通过[summary/host]菜单项对应页面中查看该主机记录，点击弹出新的页面显示此主机的具体流量等信息
IP Address	对应主机的 IP 地址
Data Sent	本地各个主机之间的发送流量情况。分别以各个对应主机发送到本地主机的流量大小和占总流量的百分比 2 种方式显示
Data Rcvd	本地各个主机之间的接收流量情况。分别以各个对应主机接收的来自本地主机的流量大小和占总流量的百分比 2 种方式显示

所有本地流量的汇总统计，参数意义如下。

表A-22 所有本地流量

表项	含义
Total Traffic	本地所有主机发送和接收的流量总和的一半（对本地流量而言，发送和接收的流量是相等的）
Data Sent	本地所有主机之间发送的流量总和
Data Rcvd	本地所有主机之间接收的流量总和
Used Bandwidth	本地主机之间通信使用的带宽

2. Local to Remote

显示了本地主机与远程主机的通信流量情况，Local to Remote IP Traffic 表显示各个本地主机的流量情况，参数意义如下。

表A-23 Local IP Traffic

表项	含义
Host	本地主机信息，如果与远程主机没有通信，则不显示。一般为主机的 IP 地址（也可以是 DNS 名称或者 NetBios 等），以蓝色超链接形式，可以通过[summary/host]菜单项对应页面中查看该主机记录，点击弹出新的页面显示此主机的具体流量等信息
IP Address	对应主机的 IP 地址
Data Sent	本地各个主机发送到远程的流量。分别以各个主机发送到远程主机的流量大小和流量所占所有流量的百分比 2 种方式显示
Data Rcvd	本地各个主机接收到远程主机的流量情况。分别以各个对应主机接收来自远程主机的流量大小和流量所占所有流量的百分比 2 种方式显示

所有本地主机流量的汇总统计，参数意义如下。

表A-24 所有本地远程流量

表项	含义
Total Traffic	所有本地主机与远程之间的流量总和
Data Sent	所有本地主机发送到远程的流量总和
Data Rcvd	所有本地主机从远程接收的流量总和
Used Bandwidth	所有本地主机与远程通信使用的带宽

3. Remote to Local

显示了远程与本网段的主机的流量情况，Remote to Local IP Traffic 表显示各远程主机的流量情况，参数意义如下。

表A-25 Remote to Local IP Traffic

表项	含义
Host	远程主机信息，如果与本地主机没有通信，则不显示。一般为主机的 IP 地址（也可以是 DNS 名称或者 NetBios 等），以蓝色超链接形式，表明 summary/host 页面中存在该主机记录，点击弹出新的页面显示此主机的具体流量统计等信息
IP Address	对应主机的 IP 地址

表项	含义
Data Sent	各个远程主机发送到本地主机之间的流量情况，分别以各个对应主机接收到本地主机的流量大小和流量所占所有流量的百分比2种方式显示
Data Rcvd	各个远程主机接收到的来自本地的流量。分别以各个对应主机接收来自本地主机流量的大小和流量所占所有流量的百分比2种方式显示

所有远程到本地的流量总和的汇总统计，参数意义如下。

表A-26 所有本地远程流量

表项	含义
Total Traffic	远程所有主机与本地主机的流量总和
Data Sent	远程所有主机发送到本地主机的流量总和
Data Rcvd	远程所有主机接收到本地主机的流量总和
Used Bandwidth	远程所有主机与本地主机通信所占带宽

4. Remote to Remote

此界面显示了远程与远程的主机的流量情况，Remote to Remote IP Traffic 表 显示各个远程主机的流量情况，参数意义如下。

表A-27 Remote to Remote IP Traffic

表项	含义
Host	远程主机信息，如果与远程主机没有通信，则不显示。一般为主机的 IP 地址（也可以是 DNS 名称或者 NetBios 等），以蓝色超链接形式，表明 summary/host 页面中存在该主机记录，点击弹出新的页面显示此主机的具体流量统计等信息
IP Address	对应主机的 IP 地址
Data Sent	各个远程主机发送到远程主机的流量情况，分别以各个对应主机接收到远程主机的流量大小和流量所占所有流量的百分比2种方式显示
Data Rcvd	各个远程主机接收到远程主机的流量。分别以各个对应主机接收的来自远程主机的流量大小和占总流量的百分比 2 种方式显示

所有远程到远程的流量汇总和统计，参数意义如下。

表A-28 所有本地远程流量

表项	含义
Total Traffic	远程所有主机与远程主机的流量总和
Data Sent	远程所有主机发送到远程主机的流量总和
Data Rcvd	远程所有主机接收到远程主机的流量总和
Used Bandwidth	远程所有主机与远程主机通信所占带宽

说明：

- 所有的流量大小单位规则如下，如果不带单位，则表示是字节数，如果流量较大，会按照流量大小以 KB、MB、或者 GB 为单位显示。
- 如果没有相应菜单没有信息，将显示 No Data To Display (yet)。

A.3.3 Local

1. Ports Used

此界面显示本地主机之间的客户端和服务器的服务类型和流量情况，分别显示主机数量和服务端口数量，以及服务所涉及到主机。

表A-29 TCP/UDP: Local Protocol Usage

表项	含义
Service	显示了服务类型和端口号
Clients	显示客户端的主机，并且用颜色标明了这个客户端第一次与服务器的连接到目前时间，可以通过单击主机查看客户端主机的详细信息
Servers	显示服务器端的主机，并且用颜色标明了这个服务器端第一次与客户端通信到目前的时间。可以通过单击主机查看服务器端的详细信息

说明：

- 如果本地主机中没有端口被使用，将显示 No Data To Display (yet)。
- 表中 client 和 server 的主机信息的颜色代表该主机第一次被捕获到报文距离到现在的时间，具体颜色参考 web 页面下的详细显示。
- 标题下方列出的 Reporting on actual traffic for xx host(s) on xx service port(s)中 host(s)表示所有本地主机的数量。

2. Active TCP Sessions

此界面显示了本地活动的 TCP 会话信息。

表A-30 Active TCP Sessions

表项	含义
Client	客户端的主机名称或 IP 地址， 端口号或者服务类型
Server	服务器端的主机名称或 IP 地址， 端口号或者服务类型
Data Sent	客户端发送到服务器端流量的值
Data Rcvd	客户端从服务器端接收流量的值
Active Since	活动开始时间
Last Seen	最后一次发现报文的时间
Duration	连接持续时间
Inactive	非活动时间
Latency	延迟时间
Note	注意信息

说明：

- 如果没有 TCP 会话，将显示 No Data To Display (yet)。
- 表中会话信息的颜色代表会话所在主机第一次被捕获到报文距离到现在的时间，具体颜色参考 web 页面下的详细显示。

3. Host Fingerprint

此界面显示了本地主机的操作系统，OS Summary 显示主机的操作系统。

OS Summary 表的含义。

表A-31 OS Summary

表项	含义
Host	主机信息。一般为主机的 IP 地址（也可以是 DNS 名称或者 NetBios 等），以蓝色超链接形式，表明 summary/host 页面中存在该主机记录，点击弹出新的页面显示此主机的具体流量统计等信息

表项	含义
其他列	分别显示不同操作系统名称，如：Windows 2000、Linux 2.4.xx 等等。 如果 Host 属于某个操作系统，则在相应的操作系统名称对应位置标记

操作系统数量统计表参数意义如下。

表A-32 操作系统数量

表项	含义
OS	操作系统的名称
Total	操作系统的数量

操作系统按照是否能够解析等具体信息细分为如下表所示各项，各参数意义如下。

表A-33 Statistics

表项		含义
Scanned	Host	所有主机数量
Less	No fingerprint	没有系统标识的主机的数量
	Broadcast	广播主机的数量
	Multicast	多播主机的数量
	Remote	远程主机的数量
	Non IP host	IP 地址为 0 的主机的数量
Gives	Possible to report	可以显示系统标识的主机数量
	Less: Can not resolve	因标识不完整而不能解析的主机数量
	Less: Unknown Fingerprint	不能解析标识即本地数据库没有对应的标识名称的主机数量

4. Hosts Characterization

此界面描述了本地主机提供了哪些服务。

表A-34 Local Hosts Characterization

表项	含义
Host	主机信息。一般为主机的 IP 地址（也可以是 DNS 名称或者 NetBios 等），以蓝色超链接形式，可以通过[summary/host]菜单项对应页面查看该主机记录，点击此主机弹出新的页面显示具体流量统计等信息

表项	含义
Unhealthy Host	服务器端的主机名称或 IP 地址
L2 Switch Bridge	对应主机是否为 2 层设备。如果是，则在相应位置下标记
Gateway	对应主机是否为网关。如果是，则在相应位置下标记
VoIP Host	是否为 voip 主机。如果是，则在相应位置下标记
Printer	对应主机是否为打印机。如果是，则在相应位置下标记
NTP/DNS Server	对应主机是否为 NTP/DNS Server。如果是，则在相应位置标记
SMTP/POP/IMAP Server	对应主机是否为邮件服务器。如果是，则在相应位置标记
Directory/FTP/HTTP Server	对应主机是否为 Directory/FTP/HTTP Server。如果是，则在相应位置标记
DHCP/WINS Server	对应主机是否为 DHCP/WINS Server。如果是，则在相应位置标记
DHCP Client	对应主机是否为 DHCP Client。如果是，则在相应位置标记
P2P	是否为 P2P 服务器，如果是，则在相应位置标记
Total	以上每种服务器的个数

5. Network Traffic Map

按照本地网络的组网图画出各个主机之间的连接关系。

6. Local Matrix

显示了本网段之间各个主机的流量情况，以矩阵的方式显示。

IP Subnet Traffic Matrix 表的每行和每列分别表示 1 个主机，以主机信息表示。

网格内容则是两台主机之间交互数据的总流量大小。

A.4 主机信息

此界面以主机为单位显示该主机的详细信息。包括主机的基本信息，如 IP、MAC、OS、数据接收和发送、最近 24 详细流量信息、发送和接收的特定协议报文的统计信息、协议分布情况、异常报文信息、端口使用情况等等。

A.4.1 Host 基本信息

表A-35 Info about Host

表项		含义
IP Address		分别显示此主机的 IP 地址、报文类型(单播、多播或广播)，同时提供锁定此主机不显示的功能
First/Last Seen		分别显示第一次捕获到报文的时间点、最后一次捕获到报文的时间点、距离现在没有捕获到报文任何报文的时间
MAC Address		该主机的 MAC 地址
Nw Board Vendor		生产厂商
OS Name		操作系统名称
Host Location		主机位置，即是 local 或者 remote
IP TTL (Time to Live)		TTL 值
Total Data Sent		发送的数据总和，分别以字节数、报文个数、重传报文数显示
Broadcast Pkts Sent		发送的广播数据总和，以包的个数来显示
Multicast Traffic		发送的多播数据总和，分别以字节数量、报文个数显示
Data Sent Stats	Local	发送数据本地流量所占比例
	Rem	发送数据远程流量所占比例
IP vs. Non-IP Sent		发送的流量中 IP 与非 IP 分别所占比例
Total Data Rcvd		接收的数据总和，分别以字节数量、报文数量、重传报文数量显示
Data Rcvd Stats		接收数据的统计，以本地流量和远程流量所占比例方式显示
IP vs. Non-IP Rcvd		接收数据中 IP 与非 IP 所占比例
Sent vs. Rcvd Pkts		发送和接收流量报文个数分别所占的比例
Sent vs. Rcvd Data		发送和接收流量字节数所占的比例
Used Subnet Routers		使用的路由器
Host Healthness (Risk Flags)		主机的风险级别
Historical Data		历史数据，点击表格右方链接可显示此主机的历史信息

说明：

- 所有流量的单位规则如下，如果不带单位，则表示是字节数；如果流量较大，会按照流量大小以 KB、MB 或者 GB 为单位显示。
- Multicast Traffic、 Used Subnet Routers、Host Healthness、Historical Data 等如果不显示，则说明主机没有这些信息。

A.4.2 Host 流量统计

表A-36 Host Traffic Stats

表项		含义
Time		以小时为单位显示
Tot. Traffic Sent		发送的流量总和
% Traffic Sent		最近二十四小时发送的流量所占百分比
Tot. Traffic Rcvd		接收的流量总和
% Traffic Rcvd		最近二十四小时接收的流量所占百分比
Total	Sent	24 小时内各小时发送的流量的分布图
	Rcvd	24 小时内各小时接收的流量的分布图

A.4.3 TCP/UDP 相关统计信息

表A-37 Packet Statistics

表项		含义
TCP Connections	Attempted	TCP 请求个数及请求的主机信息
	Established	已确定的请求个数及请求的主机信息
	Terminated	终结的请求个数及请求的主机信息
Directed to		主机发往其它主机的 TCP 请求个数及主机信息
Rcvd From		主机接收其它主机的 TCP 请求个数及主机信息

表A-38 TCP Flags

表项		含义
TCP Flags	SYN	主机发送和接收的 SYN 的个数
	RST|ACK	主机发送和接收的 RST|ACK 的个数
Pkts Sent		主机发往其他主机的 SYN 请求个数及主机信息
Pkts Rcvd		主机接收其他主机的 SYN 请求个数及主机信息

表A-39 Anomaly

表项		含义
Anomaly	UDP Pkt to Closed Port	异常信息的种类
	Closed Empty TCP Conn	异常信息的种类
	ICMP Port Unreachable	异常信息的种类

表项	含义
Pkts Sent to	主机发往其他主机的异常个数及主机信息
Pkts Rcvd from	主机接收其他主机的异常个数及主机信息

说明：

- 所有流量大小单位规则如下，如果不带单位，则表示是字节数；如果流量较大，会按照流量大小以 KB、MB 或者 GB 为单位显示。
- TCP/UDP 相关统计信息中，根据主机的通信情况显示是否有 TCP Connections、TCP Flags 和 Anomaly 等信息。如果没有，则不显示。

A.4.4 ARP 相关信息

表A-40 ARP

表项		含义
ARP	Request Sent	发送的请求的报文数量
	Reply Rcvd	收到的应答报文数量及占发送的百分比
	Reply Sent	发送的应答的报文数量
Packet		报文的数量

A.4.5 协议分布情况

表A-41 Protocol Distribution

表项	含义
Protocol	协议类型，如 TCP，UDP，ICMP，ARP 等等
Data Sent	发送的报文的数据大小
Data Rcvd	接收的报文的数据大小
Protocol Distribution	分别以发送和接受的方式显示各协议分布图
IP Distribution	分别以发送和接受的方式显示各协议分布图

A.4.6 ICMP 信息

表A-42 ICMP Traffic

表项		含义
Type	Echo Request	主机发送和接收的回显请求报文个数
	Echo Reply	主机发送和接收的回显应答报文个数
	Unreach	主机发送和接收的不可达报文个数
Pkt Sent		发送的报文个数
Pkt Rcvd		接收的报文个数

A.4.7 TCP 连接信息

表A-43 Last Contacted Peers

表项	含义
Sent To	目的主机的主机信息
IP Address	目的主机的 IP
Received From	源主机的主机信息
IP Address	源主机的 IP
Total Contacts	连其他主机的个数

A.4.8 TCP/UDP 端口应用信息

表A-44 TCP/UDP Service/Port Usage

表项	含义
IP Service	服务名称，例如 netbios-ns，snmp 等
Port	端口号
# Client Sess	该主机为客户端时发送和接受的报文个数及流量值
Last Client Peer	该主机为客户端时最后一次服务对应的服务器端的主机名称
# Server Sess	该主机为服务器时发送和接受的报文数
Last Server Peer	当本机为服务器时最后一次服务对应的客户端的主机名称

表A-45 TCP/UDP - Traffic on Other Ports

表项	含义
Client Port	本机为客户端时使用的端口号
Server Port	本机为服务器时使用的端口号

表A-46 TCP/UDP Recently Used Ports

表项	含义
Client Port	本机为客户端时使用的端口号
Server Port	本机为服务器时使用的端口号

A.5 Utils

此 Utils 功能项用于导出数据和日志的功能。

A.5.1 Data Dump

NAM 提供把网络中各主机的流量通过各种文档格式导出，供后续导入做其他处理或者查询使用。

表A-47 Data dump

表项			含义
Report Type	Hosts		所有主机信息
	Hosts Matrix		导出各个主机之间的流量情况
	NetWork Interfaces		导出监控接口的信息
	NetWork Flows		导出已经配置过的 NetFlow 信息
Description			对 Report Type 中各个子项的描述
Action	Format	text	以文本格式导出相应数据
		xml	以 xml 格式导出相应数据
		perl	以 perl 格式导出相应数据
		php	以 perl 格式导出相应数据
		python	以 python 格式导出相应数据
	Attributes List	long	以长型格式导出数据，一般只对 text 格式有区别
		short	以短型格式导出数据，一般只对 text 格式有区别
	Dump Data		点击 Dump Data 复选框导出数据

A.5.2 View Log

本页面显示系统的日志信息。

记录最近 50 条日志记录，日志级别等于或者高于 INFO。

A.6 Plugins

本菜单包含了 NAM 提供的各种插件。每个插件都有一个 Deactivate/Active 子菜单，用于关闭/激活插件，插件在激活以后才能运行它的功能。

A.6.1 Host Last Seen

本插件主要用于查看 NAM 最后一次捕获到本地局域网主机的报文的时间。

1. Deactivate/Active

关闭/启动 host last seen 功能。关闭后此菜单显示 Active，启动后此菜单显示 Deactive。

2. View

插件激活以后才显示此菜单。

用于查看主机的具体信息，包括 Host、Address、LastSeen、Comments、Options。各统计项的含义见下表。

表A-48 Last Seen Statistics

表项		含义
Host		主机信息，一般为主机的 IP 地址（也可以是 DNS 名称或者 NetBios 等） 该项一般有两种形式出现： ①蓝色超链接形式，表明[Summary/Host]页面中存在该主机记录，点击弹出新的页面显示主机的流量统计等信息； ②“-NO INFO-”形式，表明[Summary/Hos]t 页面中不存在该主机记录，NAM 已经有一段时间没捕获到该主机的报文。
Address		主机 IP 地址
LastSeen		最后一次捕获到报文的时间
Comments		说明信息，这一栏的内容可以通过点击 options 里的 Notes 编辑
Options	Del	删除主机的统计信息
	Notes	编辑 Comments 的内容

3. Describe

描述 NetFlow 插件的总体功能，当前状态，并能通过 Active[click to toggle]表项更改插件的状态。

说明：

- [Host Last Seen/View]页面显示的记录没有超时的概念，只能手工地删除记录;
- Host Last Seen 插件只记录 NAM 板卡接口所在局域网的主机信息，不会统计 NetFlow，sFlow 等虚拟 NIC 上的主机信息。
- 点击[Admin/Configure/Reset Stats]，[Host Last Seen/View]页面显示的记录不会清空。

A.6.2 ICMP Watch

本插件用于统计从网络接口捕获的各种类型的 ICMP 报文数，包括接收和发送的。

1. Deactivate/Active

关闭/启动 ICMP Watch 功能，关闭后此菜单显示 Active，启动后此菜单显示 Deactive。

2. View

插件激活以后才显示此菜单。

用于查看各种 ICMP 报文的统计信息，各统计项的含义见下表。

表A-49 ICMP Statistics

表项		含义
Host		主机信息，显示信息与 summary/host 中的有关主机的信息一致，点击后弹出新的页面显示主机的流量统计等信息
Bytes	Send	发送的 ICMP 字节数
	Rcvd	接收的 ICMP 字节数

表项		含义
Sent/Received by ICMP Type	Echo Request	主机发送和接收的回显请求报文个数
	Echo Reply	主机发送和接收的回显应答报文个数
	Time Exceed	主机发送和接收的超时报文个数
	Unreach	主机发送和接收的不可达报文个数
	Redirect	主机发送和接收的重定向报文个数
	Router Advert	主机发送和接收的路由器通告报文个数
	Param Problem	主机发送和接收的参数出错报文个数
	Network Mask	主机发送和接收的地址掩码报文个数
	Source Quench	主机发送和接收的源端被关闭报文个数
	Timestamp	主机发送和接收的时间戳请求报文个数

说明：

- 点击[Admin/Configure-/Reset Stats]，[ICMP Watch/View]页面显示的记录清空。
- ICMP Watch 插件记录当前网络接口的 ICMP 报文统计信息。所以切换网络接口会导致 ICMP 报文重新统计。

3. Describe

描述 ICMP Watch 插件的总体功能，以及当前状态，能通过 Active[click to toggle]表项更改插件的状态。

A.6.3 NetFlow

NetFlow 是一种数据交换方式，包含了数据流的统计信息，帮助网管者判断哪个主机、在什么时候、在什么地点访问了哪些站点，以便更好地规划网络、监控网络的应用和减少网络的开销。NAM 提供了 NetFlow 插件收集 NetFlow 流量以及对 NetFlow 流量进行分析。

1. Deactivate/Active

关闭/启动 NetFlow 功能，关闭后此菜单显示 Active，启动后此菜单显示 Deactive。

2. Configure

配置 Net Flow 虚拟接口的相关信息，添加，编辑和删除 NetFlow 虚拟接口。插件激活以后才能进行相关操作。

为了正确地使用 NAM 收集 NetFlow 流，使能 NetFlow 插件之后，需要添加 NetFlow 虚拟接口，并对 NetFlow 虚拟接口进行正确地配置。NetFlow 配置参数含义见下表。每个参数都有单独的按钮保存当前配置。

表A-50 NetFlow

配置参数		参数含义	参数类型
NetFlow Device（interface name）		NetFlow 虚拟接口的名称	文本框：字符串，长度 0~256
Flow Collection	Local Collector UDP Port	监听 NetFlow 数据的 UDP 端口号 只有端口号配置正确了 NAM 才能收到 NetFlow 数据，取值为 0 则不收集 NetFlow 数据	文本框：整数 缺省值是 2055，当配置的值超过 0～65535，NAM 会把值转化为 0～65535 内的值
	Virtual NetFlow Interface Network Address	NetFlow 数据源所在的网段地址 NAM 在分析 NetFlow 数据时，通过这个值判断哪些数据流是本地的，哪些数据是远端的 把该网段地址称为虚拟的，是因为 NAM 设备并没有直连到该网段	文本框：IP 网段 配置时可采用 <network>/<mask> 或者 <network>/<bits>格式， 显示时采用 <network>/<mask>格式 注意：请确保输入合法的 IP 地址。输入非法的 IP 地址不能改变现有 IP 地址，但是可能导致在一定时间内 NAM 拒绝特定主机的访问。
Flow Aggregation		NAM 可以按照各种策略对 NetFlow 统计的数据流进行聚合： Port Aggregation：按照 TCP/UDP 端口号来统计流量，忽略了具体的 IP 地址信息，采用该聚合后，如果当前 NIC 是 NetFlow 虚拟接口，[summary/hosts]等统计主机信息的页面都不会有数据显示。 Host Aggregation：按照 IP 地址来统计流量，忽略了高层信息。采用该聚合后，如果当前 NIC 是 NetFlow 虚拟接口，[IP/summary/traffic]等会统计传输层和应用层流量的页面中，传输层和应用层流量统计不会再增加 Protocol Aggregation：将流量分为 TCP、UDP、ICMP 三类，采用该聚合后，如果当前 NIC 是 NetFlow 虚拟接口，[summary/hosts]等统计主机信息的页面都不会有数据显示。[IP/summary/traffic]等会统计应用层流量的页面中，应用层流量统计不会再增加 AS Aggregation：按照 AS 号来统计流量	单选框： None TCP/UDP port Host Protocol AS

<table>
<tr><th colspan="2">配置参数</th><th>参数含义</th><th>参数类型</th></tr>
<tr><td rowspan="3">Filtering</td><td>White List</td><td>白名单列表，指明统计哪些主机或者网段的流量。
如果当前 NIC 是 NetFlow 虚拟接口，summary->hosts 等统计主机信息的页面只显示白名单列表范围内的主机。</td><td>文本框：IP 网段列表
配置时可采用 <network>/<mask> 或者 <network>/<bits>格式，
显示时采用 <network>/<bits>格式，
多个网段之间用逗号格开
注意：请确保输入合法的 IP 地址。输入非法的 IP 地址不能改变现有 IP 地址，但是可能导致在一定时间内 NAM 拒绝特定主机的访问。</td></tr>
<tr><td>Black List</td><td>黑名单列表，指明不统计哪些主机或者网段的流量。
[summary-/hosts]等统计主机信息的页面不显示黑名单列表范围内的主机。</td><td>文本框：IP 网段列表
配置时可采用 <network>/<mask> 或者 <network>/<bits>格式，
显示时采用 <network>/<bits>格式，
多个网段之间用逗号格开
注意：请确保输入合法的 IP 地址。输入非法的 IP 地址不能改变现有 IP 地址，但是可能导致在一定时间内 NAM 拒绝特定主机的访问。</td></tr>
<tr><td colspan="3">黑白名单的作用顺序如下：
如果存在黑名单，匹配黑名单主机的流量信息被丢弃
如果存在白名单，不匹配白名单主机的流量信息被丢弃
剩下的流量信息都被统计
该配置立即生效</td></tr>
<tr><td colspan="2">Assume FTP</td><td>指定 FTP 采用的是 passive 模式，在 passive 模式下，FTP data.的源和目的端口都是大于 1023 的端口号。
该配置立即生效</td><td>单选框： yes/no</td></tr>
<tr><td rowspan="3">Flow Dump</td><td>Dump Interval</td><td>把 NetFlow 数据存储到磁盘的时间间隔，每隔 Interval 会生成一个新的 FLOW 文件</td><td>文本框：整数
取 0 不存储 NetFlow 数据</td></tr>
<tr><td>Dump File Path</td><td>设置文件存储路径</td><td>文本框：文件路径名</td></tr>
<tr><td colspan="3">文件名格式如下：<time of the day>.flow
文件内容如下：[<flow length (4 digits 0 padded)><raw flow>]*</td></tr>
</table>

配置参数	参数含义	参数类型
Debug	配置是否输出 netflow 虚拟设备的 debug 信息	单选框： yes/no

说明：

- 所有未声明立即生效的参数要到 NetFlow 插件重新激活时才能生效。
- 只有正确地配置了端口号，插件才能收集到 NetFlow 数据。
- 设置 Virtual NetFlow Interface Network Address 时，请确保输入合法的 IP 地址。非法的 IP 地址不生效，同时可能导致一定时间内 NAM 拒绝特定主机的访问。
- 配置 NetFlow 参数时，务必保证参数的合法性。如果配置的参数值超过正常的范围，将自动转化为一个合法范围之内的值，例如配置 Local Collector UDP Port 时端口号超过了 65535，则自动转为一个合法范围内的端口号。
- Virtual NetFlow Interface Network Address 只能配置一个网段，如果想设置多个本地网段，需要在[Admin/Startup Options]中配置 Local Subnet Address 参数。

3. Describe

描述 NetFlow 插件的总体功能，以及当前状态，并能通过 Active[click to toggle]表项更改插件的状态。

4. Statistics

显示每个 NetFlow 虚拟设备统计信息。

表A-51 NetFlow

统计项		含义
Received Flows	Flow Senders	NetFlow 报文的发送者
	Number of Packets Received	收到的 NetFlow-报文数
	Number of Packets with Bad Version	收到错误版本号的 NetFlow 报文数
	Number of Packets Processed	提交处理的 NetFlow 报文数
	Number of Valid Flows Received	收到的有效 Flow 数
	Average Number of Flows per Packet	平均每个 NetFlow 包含的 Flow 数
	Number of V1 Flows Received	收到版本为 V1 的 Flow 数

统计项		含义
Discarded Flows	Number of V5 Flows Received	收到版本为 V5 的 Flow 数
	Number of V7 Flows Received	收到版本为 V7 的 Flow 数
	Number of V9 Flows Received	收到版本为 V9 的 Flow 数
	Number of Flows with Zero Packet Count	报文数为的 Flow 数
	Number of Flows with Zero Byte Count	字节数为零的 Flow 数
	Number of Flows with Bad Data	包含错误数据的 Flow 数
	Number of Flows with Unknown Template	包含错误模板的 Flow 数
	Total Number of Flows Processed	提交处理的 Flow 数
Accepted/ Rejected Flows	Rejected - Black list	被黑名单过滤掉的 Flow 数
	Rejected - White list	被白名单过滤掉的 Flow 数
	Accepted	接收的 Flow 数
	Total	总的 Flow 数

A.6.4 PDA

该插件用来显示用户比较关心的一些简单的统计项，包括发包数和收包数最多的主机等等。

1. Deactive/active

关闭/启动 PDA 功能，关闭后此菜单显示 Active，启动后此菜单显示 Deactive。

2. View

插件激活以后才显示此菜单。

查看 PDA 的统计信息，包括发送报文最多的主机，接受报文最多的主机，总的采样时长，单播报文百分比，广播报文百分比。

3. Describe

描述 PDA 插件的总体功能，以及当前状态，并能通过 Active[click to toggle]表项更改插件的状态。

A.6.5 Round-Robin DataBase

Round-Robin DataBase （简称 RRD），NAM 使用 RRD 数据库永久的保存一些历史流量信息。RRD 是一种按时间来保存数据的特殊数据库，而且 RRD 文件的大小不会随着时间的增加而增加。

RRD 工作原理：假设网管者要计算网络在过去十五分钟的流量，可以将网管软件设置成每分钟记录一次这一分钟的流量，那么需要十五条记录。但是如果你想要了解过去更长一段时间内的流量，数据库的大小也会随着增加。为了限制数据库的容量，只能周期性地把过去地记录删除，同时，RRD 文件包含几个不同记录区域按照不同地频率记录历史数据，包括每 interval 记录区域，每小时记录区域，每天记录区域，这样使得 RRD 使用固定的存储空间保存较久的历史流量统计而不丧失最近一段时间流量的细节。

1. Deactive/active

关闭/启动 RRD 功能。关闭后此菜单显示 Active，启动后此菜单显示 Deactive。只有 RRD 插件使能以后，NAM 才能永久地保存流量信息记录。[Summary/Network Load] 等页面的流量图都是从 RRD 文件导出的，如果 RRD 插件关闭，[Summary/Network Load]页面相应时间段的流量显示为零。RRD 插件缺省为启动状态，建议不要轻易把 RRD 插件关闭。

2. Configure

配置生成 RRD 文件所需的一些参数，参数含义如下表所示。

表A-52 RRD 文件配置参数

配置参数	参数含义	参数类型
Dump Interval	每 interval 记录区域的记录间隔，以秒为单位	文本框：整数
Throughput Granularity	Throughput RRD 文件每 interval 记录区域的记录间隔，以秒为单位。 该值对应 throughput RRD 文件的记录间隔。修改以后 throughput RRD 文件的历史记录将清空。Summary->Network Load 页面的流量图是从 throughput RRD 文件导出的。	文本框：整数
Dump Hours	保存每 interval 历史记录的小时数 超过该时间范围的每 interval 历史记录将会覆盖最早的每 interval 历史记录。	文本框：整数
Dump Days	保存每小时历史记录的天数 超过该时间范围的每小时历史记录将会覆盖最早的每小时历史记录。	文本框：整数

配置参数	参数含义	参数类型
Dump Months	保存每天历史记录的月数 超过该时间范围的每天历史记录将会覆盖最早的每天历史记录。	文本框：整数
RRD Update Delay	RRD 文件更新的间隔，以毫秒为单位。 需要更新的 RRD 文件很多时，长间隔会影响 RRD 插件的性能	文本框：整数
Data to Dump	要保存 RRD 文件的数据类型 Domains：保存各个域的历史流量数据 Flows：保存各种流的历史流量数据 Hosts：保存各个主机的历史流量数据 Interfaces：保存各个接口的历史流量数据 Matrix：保存各主机之间的历史流量数据	多选框：Domains/ Flows/ Hosts/ Interfaces/ Matrix
Hosts Filter	主机过滤列表 只保存匹配主机过滤列表的主机历史流量数据，为空则保存所有主机的历史流量数据	文本框：IP 网段列表 配置时可采用 <network>/<mask> 或者 <network>/<bits>格式， 多个网段之间用逗号格开 注意：请确保输入合法的 IP 地址。输入非法的 IP 地址可能导致在一定时间内 NAM 拒绝特定主机的访问。

配置参数	参数含义	参数类型
RRD Detail	历史流量信息的详细程度 Low：仅统计 pktSent/pktRcvd、bytesSent/bytesRcvd Medium：增加下面各项的统计 pktDuplicatedAckSent/pktDuplicated AckRcvd、pktBroadcastSent、bytesBroadcastSent、pktMulticastSent、bytesMulticastSent、pktMulticastRcvd、bytesMulticastRcvd、bytesSentLoc、bytesSentRem、bytesRcvdLoc、bytesRcvdFromRem、ipBytesSent、ipBytesRcvd、tcpSentLoc、tcpSentRem、tcpRcvdLoc、tcpRcvdFromRem、tcpFragmentsSent,、cpFragmentsRcvd、udpSentLoc、udpSentRem、udpRcvdLoc、udpRcvdFromRem、udpFragmentsSent、udpFragmentsRcvd、icmpSent、icmpRcvd、icmpFragmentsSent、icmpFragmentsRcvd、ipv6Sent、ipv6Rcvd、NonIP、stpSent、stpRcvd、ipxSent、ipxRcvd、osiSent、osiRcvd、dlcSent、dlcRcvd、arp_rarpSent、arp_rarpRcvd、arpReqPktsSent、arpReplyPktsSent、arpReplyPktsRcvd、decnetSent、decnetRcvd、appletalkSent、appletalkRcvd、netbiosSent、netbiosRcvd、otherSent、otherRcvd 以及应用层协议的 Sent/Rcvd Full ：增加下面各项的统计 totContactedSentPeers、totContactedRcvdPeers 以及应用层协议的 Sent/Rcvd，比如 IP_HTTP	单选框：Low/Medium/Full

配置参数	参数含义	参数类型
RRD Files Path	RRD 文件的存放路径 RRD 文件存放在该路径的各个子文件夹下，路径名不能包含“.”，否则系统无法识别	文本框：路径名称 缺省值为“/usr/local/var/ntop/rrd”
File/Directory Permissions	RRD 文件夹访问权限 Private：仅 NAM 登录用户可以访问 Group：仅 NAM 登录用户所在组成员可以访问 Everyone：任何用户都可以访问 访问权限仅对新生成的 RRD 文件或者新登录的用户有效，已登录的用户保持修改前的访问权限	单选框：Private/ Group/ Everyone

3. Describe

描述 RRD 插件的总体功能，以及当前状态，并能通过 Active[click to toggle]表项更改插件的状态。

4. Statistics

显示 RRD 的统计信息，包括 Cycles、File Updated、Updated Errors、Graphic Requests，各表项含义解释如下表。

表A-53 RRD Statistics

表项	含义
Cycles	周期数，每经过 Dump interval，周期数增加 1
Files Updated	文件更新的总次数
Updated Errors	文件更新时生成的错误数
Graphic Requsets	请求生成流量图的次数

5. Arbitrary Graphs

通过此页面可以对已经存在的 RRD 文件进行导出流量图，数据表格等操作，进行导出操作以前做必要的配置，配置参数含义说明如下表。

表A-54 RRD 导出配置参数

配置参数	参数含义	参数类型
Action	对 RRD 文件进行的操作 Create the graph：导出流量图 Display the url to request the graph：导出流量图的 url Retrieve rrd data in table form：导出 RRD 文件的数据，以表格形式显示 Retrieve rrd data as CSV：导出 RRD 文件的数据，以 CSV 形式显示	单选框：Create the graph/ Display the url to request the graph/ Retrieve rrd data in table form/ Retrieve rrd data as CSV
File	具体的 RRD 文件	下拉列表：包含所有可能的 RRD 文件
Interface	设置需导出历史数据的设备，包括 eth0，NetFlow，Sflow	单选框
Host IP address	设置需导出历史数据的主机 IP 地址	文本框： IP 地址
Start	历史数据的起始时间 不填则取 end-1d 取 0 则从最早的记录开始	可以用下面表示方法 类似 Oct 12， 10/12/2005 等易理解的格式. 相对时间：如 now-1d，now-5mon1w2d 从 epoch 经过的秒数：如 1110286800 等价于 Tue 08 Mar 2005 07:00:00 AM CST 注意：请确保输入合法的 IP 地址。可能导致在一定时间内 NAM 拒绝特定主机的访问。
End	历史数据的结束时间	可以用下面表示方法 类似 Oct 12， 10/12/2005 等易理解的格式. 相对时间：如 now-1d，now-5mon1w2d 从 epoch 经过的秒数：如 1110286800 等价于 Tue 08 Mar 2005 07:00:00 AM CST
Legend	对统计计量的说明，比如流量图显示的是字节数，就可以把 Legend 设置为 bytes 仅当 action 选择 Create the graph 时有效	文本框：字符串

配置参数	参数含义	参数类型
Title to appear above the graph	流量图的标题 仅当 action 选择 Create the graph 时有效	文本框：字符串

配置完参数以后，单击<Make Request>按钮生成所需要的东西。

A.6.6 sFlow

sFlow（RFC 3176）是基于标准的最新网络导出协议，能够解决当前网络管理人员面临的很多问题。与使用镜像端口、探针和旁路监测技术的传统网络监视解决方案相比，sFlow 能够明显地降低实施费用，同时可以使面向每一个端口的全企业网络监视解决方案成为可能。sFlow 是一种导出格式，它增加了关于被监视数据包的更多信息，并使用嵌入到网络设备中的 sFlow 代理转发被采样数据包，因此在功能和性能上都超越了当前使用的 RMON、RMON II 和 NetFlow 技术。NAM 提供了 sFlow 插件收集 sFlow 流量以及对 sFlow 流量进行分析。

1. Deactive/active

关闭/启动 sFlow 功能。关闭后此菜单显示 Active，启动后此菜单显示 Deactive

2. View/Configure

配置 sFlow 虚拟接口的相关信息，添加，编辑和删除 sFlow 虚拟接口。插件激活以后才能进行相关操作。

为了正确地使用 NAM 收集 sFlow 流，使能 sFlow 插件之后，需要添加 sFlow 虚拟接口，并对 sFlow 虚拟接口进行正确地配置。sFlow 配置参数含义见下表，每个参数都有单独的按钮保存当前配置。

表A-55 sFlow 配置参数

配置参数		参数含义	参数类型
sFlow Device（interface name）		sFlow 虚拟接口的名称	文本框：字符串，长度 0~256
Flow Collection	Local Collector UDP Port	监听 sFlow 数据的 UDP 端口号 只有端口号配置正确了NAM才能收到sFlow数据，取值为0则不收集sFlow数据，	文本框：整数 默认值是 6343，当配置的值超过0～65535，NAM 会把值转化为 0～65535 内的值
	Virtual sFlow Interface NetworkAddress	sFlow数据源所在的网段地址，NAM 在分析 sFlow 数据时，通过这个值判断哪些数据流是本地的，哪些数据是远端的 之所以把该网段地址成为虚拟的，是因为 NAM 设备并没有直连到该网段	文本框： IP 网段 配置时可采用<network>/<mask>或者<network>/<bits>格式， 显示时采用<network>/<mask>格式 注意：请确保输入合法的 IP 地址。输入非法的IP地址不能改变现有IP地址，但是可能导致在一定时间内NAM 拒绝特定主机的访问。
Filtering	White List	白名单列表，指明统计哪些主机或者网段的流量，如果当前 NIC 是 sFlow 虚拟设备，[summary/hosts]等统计主机信息的页面只显示白名单列表范围内的主机。	文本框： IP 网段列表 配置时可采用<network>/<mask>或者<network>/<bits>格式， 显示时采用<network>/<bits>格式， 多个网段之间用逗号格开 注意：请确保输入合法的 IP 地址。输入非法的IP地址不能改变现有IP地址，但是可能导致在一定时间内NAM 拒绝特定主机的访问。
	Black List	黑名单列表，指明不统计哪些主机或者网段的流量。[summary/lhosts]等统计主机信息的页面不显示黑名单列表范围内的主机	文本框： IP 网段列表 配置时可采用<network>/<mask>或者<network>/<bits>格式， 显示时采用<network>/<bits>格式， 多个网段之间用逗号格开 注意：请确保输入合法的 IP 地址。输入非法的IP地址不能改变现有IP地址，但是可能导致在一定时间内NAM 拒绝特定主机的访问。
	黑白名单的作用顺序如下： 如果存在黑名单，匹配黑名单主机的流量信息被丢弃 如果存在白名单，不匹配白名单主机的流量信息被丢弃 剩下的流量信息都被统计 该配置立即生效		
Debug		配置是否输出 sFlow 虚拟接口的 debug 信息	-

说明：

- 所有未声明立即生效的参数要到 sFlow 插件重新激活时才能生效。
- 只有正确地配置了端口号，插件才能收集到 sFlow 数据。
- 设置 Virtual sFlow Interface Network Address 时，请确保输入合法的 IP 地址。非法的 IP 地址不生效，同时可能导致一定时间内 NAM 拒绝特定主机的访问。
- Virtual sFlow Interface Network Address 只能配置一个网段，如果想设置多个本地网段，需要在[Admin/Startup Options]中配置 Local Subnet Address 参数。

3. Describe

描述 sFlow 插件的总体功能，以及当前状态，并能通过 Active[click to toggle]表项更改插件的状态。

A.6.7 All

All 页面将各个插件的 Describe 页面显示的信息集中，便于查看各个插件当前的状态。

A.7 Admin

Admin 菜单包含三个子菜单项：[Switch NIC][Configure][shutdown]，分别用来切换网络接口，更改 NAM 系统级配置，关闭 NAM 进程。

A.7.1 Switch NIC

本菜单用于切换网络接口，切换以后，[Summary]、[All Protocols]、[IP]菜单显示的新的网络接口数据，NAM 还是会监控防火墙网络接口的流量。默认情况下，[Summary]、[All Protocols]、[IP]菜单各子菜单项显示的均为 eth0 的统计数据。

Switch NIC 按钮切换网络接口，Reset 将单选框的选择复位。

A.7.2 Configure

本菜单用于更改 NAM 系统级配置，包括下次启动的配置参数，当前的配置参数，以及安全策略等等。第一次进入 Configure 菜单需要登录，缺省的用户名密码均为 admin。

1. Startup Options

配置 NAM 下次启动时使用的配置参数，配置参数分四大类：Basic Preferences、Display Preferences、IP Preferences、Advanced Preferences。下面对各类参数的具体含义进行说明。

表A-56 Basic Preferences 配置参数

配置参数	参数含义	参数类型
Capture Interfaces (-i)	指定用于监控流量的本地接口 如果没有指定任何接口，默认选择多选框列表的第一个以太网口	多选框 该多选框会把所有的本地接口和 loopback 显示出来以供选择
Capture File Path (-f)	指定从文件里读取报文数据，而不监控本地接口流量， 配置此参数后，NetFlow，sFlow 仍然有效。 缺省配置为不从文件读取报文数据	文本框：文件路径＋文件名
Capture Filter Expression (-B)	指定 NAM 本地接口监控的流量类型，缺省情况下，监控所有类型的流量。	文本框：BPF 表达式
Packet sampling rate (-C)	指定采样比例, 每几个报文采一个进行统计, 缺省为 1, 全部采样, 若为 2, 则表示采样 50%, 依此类推	文本框：整数
Enable Session Handling (-z)	使能 TCP session 跟踪 使能以后，[IP/Local]菜单增加 Active TCP/UDP session 子菜单 缺省为使能 TCP session 跟踪	单选框：Yes/no
Enable Protocol Decoders (-b)	使能协议分析器 协议分析器检测分析协议的部分数据内容包括 NetBIOS，Netware SAP 等二层协议以及 DNS， http，ftp 等应用层协议，具体包含以下内容： DNS Sniffing：对 DNS 内容的探测，保存域名 NetBIOS， NetWare，AppleTalk，bootp/dhcp，OSI ：探测内容，记录有用资源 http (80)：记录 Request 请求成功或者失败次数等 ftp：passive 模式的跟踪，获取 ftp-data 使用的端口号 Wrong Port：监测 http，ftp，smtp 等协议是否使用错误端口号，并记录到可疑文件里 缺省为使能协议分析器	单选框：Yes/no

配置参数	参数含义	参数类型
Flow Spec (-F)	定义特定的流 格式为：<flow-label>='<matching expression>'[,<flow-label>='<matching expression>'] 缺省情况下，不配置特定流	文本框：流定义格式
Local Subnet Address (-m)	一个内部网络往往包含很多网段，该参数用来添加本地子网网段 缺省情况下，不添加网段	文本框： IP 网段列表 多个网段之间用逗号格开
Sticky Hosts (-c)	配置如果经过一段时间没有收到主机的报文，是否将主机从内存清除 内存中保存了很多主机的统计信息，为了节省内存资源，可以周期性地将这些信息清除 缺省情况下，不删除主机信息	单选框：Yes/no
Track Local Hosts (-g)	只监控本地主机 本地主机包含 Local Subnet Address (-m)指定网段的所有主机。 缺省情况下，监控本地和远端的主机。	单选框：Yes/no
Disable Promiscuous Mode (-s)	禁用网卡的混杂模式 缺省为不禁用混杂模式	单选框：Yes/no

表A-57 Display Preferences 配置参数

配置参数	参数含义	参数类型
Refresh Time (-r)	网页刷新的周期，缺省值为 120 秒	文本框：整数
Max Table Rows (-e)	网页上表格的最大行数，超过则分页显示，缺省值为 128	文本框：整数
No Info On Invalid LUNs	对不存在的 LUNs，不给出提示信息，缺省情况下，给出提示信息	单选框：Yes/no
Use W3C	采用 W3C 兼容格式，缺省为采用	单选框：Yes/no

表A-58 IP Preferences 配置参数

配置参数	参数含义	参数类型
Use IPv4 or IPv6 (-4/-6)	指定 web 服务器响应哪种地址族的请求 缺省情况下，响应 IPv4 和 IPv6 请求	单选框：IPv4/IPv6/Both
Local Domain Name (-D)	指定本地域名	文本框：字符串
No DNS (-n)	不保存 IP 地址的域名 缺省为保存域名	单选框：Yes/no
TCP/UDP Protocols To Monitor (-p)	指定监控的应用层协议，缺省情况下监控以下应用层协议： FTP = ftp | ftp-data HTTP = http | www | https | 3128 DNS = name | domain Telnet = telnet | login NBios-IP = netbios-ns | netbios-dgm | netb-ios-ssn Mail = pop-2 | pop-3 | pop3 | kpop | smtp | imap | imap2 DHCP-BOOTP = 67-68 SNMP = snmp | snmp-trap NNTP = nntp NFS = mount | pcnfs | bwnfs | nfsd | nfsd-stat-us X11 = 6000-6010 SSH = 22 Peer-to-Peer Protocols ---------------------- Gnutella = 6346 | 6347 | 6348 Kazaa = 1214 WinMX = 6699 | 7730 DirectConnect = 0 eDonkey = 4661-4665 BT = 6969|6889 ---------------------- Instant Messenger(Messenger) = 1863 | 5000 | 5001 | 5190-5193	文本框：<label>=<protocol list> [, <label>=<protocol list>],
P3P-CP	指定响应 P3P 策略头的值	文本框
P3P-URI	指定响应 P3P URL 信息的值	文本框
Host Mapper URL (-U)	配置主机的 URL 信息	文本框

表A-59 Advanced Preferences 配置参数

配置参数	参数含义	参数类型
Max Hashes (-x)	内存中存储的最大主机数，缺省值为 8192	文本框：整数
Max Sessions (-X)	内存中保存的最大 TCP 连接数，缺省值为 32768	文本框：整数
Don't Merge Interfaces (-M)	不将所有 NIC 的流量统计到一起。存在 NetFlow，sFlow 虚拟接口的情况下，各 NIC 的流量分别统计，不受该参数影响	单选框：Yes/no
No Instant Session Purge	清除已经完成的 TCP 会话的记录 缺省为清空过时的 TCP 会话记录	单选框：Yes/no
Set Pcap to Nonblocking	把 Pcap 设置成不阻塞 缺省为不设置成不阻塞	单选框：Yes/no
No web on memory error	当内存出错时，显示空白页面 缺省为显示空白页面	单选框：Yes/no
Don't Trust MAC Address (-o)	不保存本地主机的 MAC 地址 缺省为保存本地主机 MAC 地址	单选框：Yes/no
Pcap Log Base Path (-O)	捕获的报文存放的路径 缺省情况下未配置	文本框：文件路径
Use SSL Watchdog	开启 SSL 看门狗功能 缺省为不开启看门狗功能	单选框：Yes/no
Disable SchedYield	禁止 SchedYield 调用 启用 SchedYield 调用会提高 NAM 工作性能，但是在一些情况下会导致死锁 缺省为禁止 SchedYield 调用	单选框：Yes/no

2. Preferences

该页面把 NAM 可配置的参数以点分形式列出来，方便使用，下面列出 Preferences 点分式的参数与其他参数的对应关系。

表A-60 Preferences 配置参数

参数	对应配置项
actualReportDeviceId	Admin/Switch NIC
ntop.accessLogFile	Admin/Configure/Startup Options/Debugging Preferences/ Log HTTP Requests

参数	对应配置项
ntop.daemonMode	Admin/Configure/Startup Options/Basic Preferences/ Run as daemon
ntop.debugMode	Admin/Configure/Startup Options/ Debugging Preferences/ Run in debug mode
ntop.devices	Admin/Configure/Startup Options/ Basic Preferences/
ntop.disableInstantSessionPurge	Admin/Configure/Startup Options/Advanced Preferences/ No Instant Session Purge
ntop.disableMutexExtraInfo	Admin/Configure/Startup Options/ Debugging Preferences/ Disable Extra Mutex Info
ntop.disablePromiscuousMode	Admin/Configure/Startup Options/ Basic Preferences/ Disable Promiscuous Mode
ntop.disableStopcap	Admin/Configure/Startup Options/
ntop.dontTrustMACaddr	Admin/Configure/Startup Options/ Advanced Preferences/ Don't Trust MAC Address
ntop.enableOtherPacketDump	Admin/Configure/Startup Options/ Debugging Preferences/ Save Other Packets
ntop.enablePacketDecoding	Admin/Configure/Startup Options/ Basic Preferences/ Enable Protocol Decoders
ntop.enableSessionHandling	Admin/Configure/Startup Options/ Basic Preferences/ Enable Session Handling
ntop.enableSuspiciousPacketDump	Admin/Configure/Startup Options/ Debugging Preferences/ Save Suspicious Packets
ntop.flowSpecs	Admin/Configure/Startup Options/ Basic Preferences/ Flow Spec
ntop.ipv4orv6	Admin/Configure/Startup Options/IP Preferences/ Use IPv4 or IPv6
ntop.localAddresses	Admin/Configure/Startup Options/ Basic Preferences/ Local Subnet Address
ntop.maxNumHashEntries	Admin/Configure/Startup Options/ Advanced Preferences/ Max Hashes
ntop.maxNumLines	Admin/Configure/Startup Options/Display Preferences/ Max Table Rows
ntop.maxNumSessions	Admin/Configure/Startup Options/ Advanced Preferences/ Max Sessions
ntop.mergeInterfaces	Admin/Configure/Startup Options/ Advanced Preferences/ Don't Merge Interfaces
ntop.noInvalidLunDisplay	Admin/Configure/Startup Options/ Display Preferences/ No Info On Invalid LUNs
ntop.numericFlag	Admin/Configure/Startup Options/ IP Preferences/ No DNS

参数	对应配置项
ntop.pcapLogBasePath	Admin/Configure/Startup Options/ Advanced Preferences/ Pcap Log Base Path
ntop.printFcOrIp	Admin/Configure/Startup Options/ Display Preferences/ Show Menus For
ntop.refreshRate	Admin/Configure/Startup Options/ Display Preferences/ Refresh Time
ntop.sampleRate	Admin/Configure/Startup Options/ Basic Preferences/ Packet sampling rate
ntop.schedYield	Admin/Configure/Startup Options/ Advanced Preferences/ Disable SchedYield
ntop.setNonBlocking	Admin/Configure/Startup Options/ Advanced Preferences/ Set Pcap to Nonblocking
ntop.sslPort	Admin/Configure/Startup Options/ Basic Preferences/ HTTPS Server
ntop.stickyHosts	Admin/Configure/Startup Options/ Basic Preferences/ Sticky Hosts
ntop.traceLevel	Admin/Configure/Startup Options/ Debugging Preferences/ Trace Level
ntop.trackOnlyLocalHosts	Admin/Configure/Startup Options/ Basic Preferences/ Track Local Hosts
ntop.useSSLwatchdog	Admin/Configure/Startup Options/ Advanced Preferences/ Use SSL Watchdog
ntop.useSyslog	Admin/Configure/Startup Options/ Debugging Preferences/ Use Syslog
ntop.w3c	Admin/Configure/Startup Options/ Display Preferences/ Use W3C
ntop.webPort	Admin/Configure/Startup Options/ Basic Preferences/ HTTP Server
pluginStatus.Host Last Seen	Plugins/Host Last Seen/Deactive(Active)
pluginStatus.ICMP Watch	Plugins/ ICMP Watch/Deactive(Active)
pluginStatus.NetFlow	Plugins/ NetFlow/Deactive(Active)
pluginStatus.PDA	Plugins/ PDA /Deactive(Active)
pluginStatus.Round-Robin Databases	Plugins/ Round-Robin Databases/Deactive(Active)
pluginStatus.sFlow	Plugins/ sFlow /Deactive(Active)
pluginStatus.SNMP	Plugins/ SNMP/Deactive(Active)
netflow.X.blackList	Plugins/ NetFlow/Configure/Edit NetFlow Device/Set Black List
netflow.X.debug	Plugins/ NetFlow/Configure/Edit NetFlow Device/ Set Debug
netflow.X.humanFriendlyName	Plugins/ NetFlow/Configure/Edit NetFlow Device/ Set Interface Name

参数	对应配置项
netflow.X.ifNetMask	Plugins/ NetFlow/Configure/Edit NetFlow Device/ Set Interface Address
netflow.X.netFlowAggregation	Plugins/ NetFlow/Configure/Edit NetFlow Device/ Set Aggregation Policy
netflow.X.netFlowAssumeFTP	Plugins/ NetFlow/Configure/Edit NetFlow Device/ Set FTP Policy
netflow.X.netFlowDumpInterval	Plugins/ NetFlow/Configure/Edit NetFlow Device/ Set Dump Interval
netflow.X.netFlowDumpPath	Plugins/ NetFlow/Configure/Edit NetFlow Device/ Set Dump File Path
netflow.X.netFlowInPort	Plugins/ NetFlow/Configure/Edit NetFlow Device/ Set Port
netflow.X.whiteList	Plugins/ NetFlow/Configure/Edit NetFlow Device/ Set White List
rrd.dataDumpDays	Plugins/ Round-Robin Databases/ Configure/ Dump Days
rrd.dataDumpDetail	Plugins/ Round-Robin Databases/ Configure/ RRD Detail
rrd.dataDumpDomains	Plugins/ Round-Robin Databases/ Configure/ Data to Dump
rrd.dataDumpFlows	Plugins/ Round-Robin Databases/ Configure/ Data to Dump
rrd.dataDumpHosts	Plugins/ Round-Robin Databases/ Configure/ Data to Dump
rrd.dataDumpHours	Plugins/ Round-Robin Databases/ Configure/ Dump Hours
rrd.dataDumpInterfaces	Plugins/ Round-Robin Databases/ Configure/ Data to Dump
rrd.dataDumpInterval	Plugins/ Round-Robin Databases/ Configure/ Dump Interval
rrd.dataDumpMatrix	Plugins/ Round-Robin Databases/ Configure/ Data to Dump
rrd.dataDumpMonths	Plugins/ Round-Robin Databases/ Configure/ Data to Dump
rrd.dumpShortInterval	Plugins/ Round-Robin Databases/ Configure/ Throughput Granularity
rrd.hostsFilter	Plugins/ Round-Robin Databases/ Configure/ Hosts Filter
rrd.permissions	Plugins/ Round-Robin Databases/ Configure/ File/Directory Permissions
rrd.rrdDumpDelay	Plugins/ Round-Robin Databases/ Configure/ RRD Update Delay
rrd.rrdPath	Plugins/ Round-Robin Databases/ Configure/ RRD Files Path

参数	对应配置项
sflow.X.blackList	Plugins/ sFlow/Configure/Edit sFlow Device/Set Black List
sflow.X.debug	Plugins/ sFlow/Configure/Edit sFlow Device/Set Debug
sflow.X.ifNetMask	Plugins/ sFlow/Configure/Edit sFlow Device/Set Interfaces Address
sflow.X.sflowAggregation	无
sflow.X.sflowAssumeFTP	无
sflow.X.sflowInPort	Plugins/ sFlow/Configure/Edit sFlow Device/Set Port
sflow.X.whiteList	Plugins/ sFlow/Configure/Edit sFlow Device/Set White List
sflow.knownDevices	无

说明：

- 把参数的值设置成空会把该配置行删除。
- 可以自定义主机组，方法为 cluster.<name>=<network list>。比如：cluster.Home=192.168.0.0/16,172.0.0.0/8
- 可以自定义 VLAN ID 和 VLAN 名称的映射，方法为 vlan.<vlan id>=<vlan name>。比如：vlan.10=Administration.

3. Packet Filter

配置当前的过滤规则，Old Filter Expression 显示旧的过滤规则，New Filter Expression 配置新的过滤规则，使用 BPF 格式，点击 Change Filter 按钮后，配置立即生效。

4. Reset stats

清空内存中的统计数据，包括主机信息，TCP 连接信息，各种流量的统计等等。

5. Web Users

对 Web 用户进行管理，具有相关权限的用户才能访问对应的页面。进入 Web Users 菜单后以表格形式显示已经注册的用户。

单击 ，修改用户密码。单击 ，删除用户。

单击[Add User]，添加用户。

6. Protected URLs

一些页面，比如[Admin/Configure/Startup options]，涉及到 NAM 进程的配置。如果所有用户都可以对配置修改，会产生无法估计的错误。于是将这些页面保护起来，具有权限的用户才可以访问。Protected URLs 对受保护的页面进行管理，进入 Protected URLs 菜单后显示所有受保护的页面。

单击，修改页面的授权用户。单击，删除受保护页面。

单击[Add URL]，添加受保护页面。

A.7.3 Shutdown

关闭 NAM 进程。